*GFI Product Manual*

# GFI EndPointSecurity™

# *Konfigurations- und Administrationshandbuch*





http://www.gfi.com

info@gfi.com

Die Informationen in diesem Dokument dienen ausschließlich Informationszwecken und werden in der vorliegenden Form ohne (ausdrückliche oder stillschweigende) Haftung jeglicher Art bereitgestellt, insbesondere ohne Gewährleistung der Marktgängigkeit, der Eignung für einen bestimmten Zweck oder der Nichtverletzung von Rechten. GFI Software haftet nicht für etwaige Schäden, einschließlich Folgeschäden, die sich aus der Nutzung dieses Dokuments ergeben. Die Informationen stammen aus öffentlich zugänglichen Quellen. Trotz sorgfältiger Prüfung der Inhalte übernimmt GFI keine Haftung für die Vollständigkeit, Richtigkeit, Aktualität und Eignung der Daten. Des Weiteren ist GFI nicht für Druckfehler, veraltete Informationen und Fehler verantwortlich. GFI übernimmt keine Haftung (ausdrücklich oder stillschweigend) für die Richtigkeit oder Vollständigkeit der in diesem Dokument enthaltenen Informationen.

Nehmen Sie mit uns Kontakt auf, wenn Ihnen in diesem Dokument Sachfehler auffallen. Wir werden Ihre Hinweise sobald wie möglich berücksichtigen.



Zuletzt aktualisiert: 6 September 2011
Version: ESEC-ACM-DE-02.00.01

# Inhalt

# Abbildungsverzeichnis

# 1 Einführung

## 1.1 Informationen zu tragbaren Speichermedien und ihren Gefahren

Der Hauptvorteil von tragbaren Speichermedien besteht in ihrer einfachen Handhabung und der schnellen Zugänglichkeit. Theoretischerweise ist dies ein großer Vorteil für Organisationen. Es zeigt sich jedoch auch immer wieder, dass ein Datentransfer auf diesem Weg auf Kosten der Sicherheit geht, sofern keine Schutzmaßnahmen implementiert sind.

Die Entwicklung tragbarer Speichermedien schreitet rasant voran, und aktuelle mobile Massenspeicher bieten immer mehr Speicherplatz und eine höhere Leistung. Neuere Versionen tragbarer Speichermedien, wie Flash, haben sich hinsichtlich Folgendem verbessert:

» Höhere Speicherkapazität

» Verbesserte Leistung

» Einfachere und schnellere Installation

» Kompakte Abmaße, die für höchste Mobilität sorgen.

Netzwerkinterne Anwender können somit (ob nun wissentlich oder unabsichtlich):

» vertrauliche Daten entwenden,

» vertrauliche Daten veröffentlichen,

» böswilligen Code einschleppen (z. B. Viren oder Trojaner), der den gesamten Netzwerkbetrieb zum Erliegen bringt,

» unerwünschte oder beleidigende Inhalte auf Unternehmensrechner überspielen,

» persönliche Kopien von Unternehmensdaten und geistigem Eigentum anfertigen und

» von produktivem Arbeiten abgehalten werden.

Mehr und mehr Firmen stellen Richtlinien auf, die den Einsatz (privater) tragbarer Speichermedien am Arbeitsplatz verhindern sollen. In der Praxis zeigt sich, das man sich nicht auf eine freiwillige Einhaltung durch die Mitarbeiter verlassen kann. Nur durch den Einsatz technologischer Sperren lässt sich die Verwendung tragbarer Medien im Netzwerk umfassend kontrollieren.

## 1.2 GFI EndPointSecurity - die Lösung

GFI EndPointSecurity sichert die Integrität von Daten und verhindert den unautorisierten Zugriff auf tragbare Speichermedien sowie den Datenaustausch auf und von folgender Hardware und Schnittstellen:

» USB-Schnittstellen (z. B. Speicherkartenleser und USB-Sticks)

» FireWire-Schnittstellen (z. B. Digitalkameras, FireWire-Kartenleser)

» Funkschnittstellen (z. B. Bluetooth- und Infrarot-Dongle)

» Diskettenlaufwerke (intern und extern)

» Optische Laufwerke (z. B. CD, DVD)

» Optische MO-Laufwerke (intern und extern)

» USB-Festplattenlaufwerke

» Andere Laufwerke wie Zip- und Bandlaufwerke (intern und extern).

GFI EndPointSecurity ermöglicht es Ihnen, den Zugriff zu erlauben oder zu sperren und darüber hinaus volle Zugriffsrechte oder allein Leserechte zu erteilen für:

- Geräte (z. B. CD-/DVD-Laufwerke, PDAs)
- Lokale oder Active Directory-Benutzer/-Benutzergruppen.

Der Zugriff auf sämtliche mobile Geräte, die an kontrollierte Computer angeschlossen werden, lässt sich zudem mit Informationen zu Datum und Uhrzeit der Verwendung sowie zum Gerätebenutzer protokollieren.

## 1.3 Dieses Handbuch

Dieses Benutzerhandbuch ist eine umfassende Anleitung, die bei der Erstellung und Bereitstellung von GFI EndPointSecurity-Schutzrichtlinien helfen soll. Es beschreibt die Nutzung und Konfiguration von GFI EndPointSecurity, um die bestmögliche Unternehmenssicherheit zu erreichen.

Dieses Handbuch enthält folgende Kapitel:

| | |
|---|---|
| **Kapitel 1** | **Einführung**<br>Einführung in dieses Handbuch |
| **Kapitel 2** | **Informationen zu GFI EndPointSecurity**<br>Grundlegende Informationen zu GFI EndPointSecurity und dessen Funktionsweise |
| **Kapitel 3** | **Erstellen neuer Schutzrichtlinien**<br>Informationen zur Erstellung neuer Schutzrichtlinien mithilfe des Assistenten zur Erstellung von Schutzrichtlinien |
| **Kapitel 4** | **Bereitstellen von Schutzrichtlinien**<br>Informationen zur Bereitstellung von Schutzrichtlinien auf zu kontrollierenden Computern |
| **Kapitel 5** | **Überwachen der Geräteaktivität**<br>Informationen zur Aktivitätsüberwachung von Geräten und Schnittstellen auf kontrollierten Computern |
| **Kapitel 6** | **Statusüberwachung**<br>Informationen zur Statusüberwachung von bereitgestellten Agenten auf kontrollierten Computern |
| **Kapitel 7** | **Berichterstattung**<br>Informationen zur Informationssammlung über GFI EndPointSecurity ReportPack |
| **Kapitel 8** | **Erkennen von Geräten**<br>Informationen zur Erkennung und Meldung aller Geräte, die an kontrollierten Computern angeschlossen sind und waren |
| **Kapitel 9** | **Anpassen von Schutzrichtlinien**<br>Informationen zur Konfiguration von Schutzrichtlinieneinstellungen |
| **Kapitel 10** | **Anpassen von GFI EndPointSecurity**<br>Informationen zur Anpassung von GFI EndPointSecurity-Einstellungen |
| **Kapitel 11** | **Deinstallation von GFI EndPointSecurity**<br>Informationen zur Deinstallation von GFI EndPointSecurity-Agenten und der GFI EndPointSecurity-Anwendung |
| **Kapitel 12** | **Diverses**<br>Informationen zur Lizenzierung und Versionsverwaltung |
| **Kapitel 13** | **Fehlerbehebung**<br>Alle notwendigen Informationen zur Handhabung von Fehlern, die bei der Verwendung von GFI EndPointSecurity auftreten können. Außerdem stehen umfassende Supportinformationen zur Verfügung. |
| **Kapitel 14** | **Glossar**<br>Definition von technischen Begriffen, die innerhalb von GFI EndPointSecurity verwendet werden |
| **Kapitel 15** | **Anhang 1 - Bereitstellungsfehlermeldungen**<br>Liste von Fehlern, die während der Bereitstellung von Agenten durch die Verwaltungskonsole angezeigt werden können |

*Erste Schritte*

Im **GFI EndPointSecurity - Erste Schritte** finden Sie Installationshinweise. Diese Anleitung können Sie von der GFI-Website herunterladen:

**http://www.gfisoftware.de/esec/esec4gettingstartedguide_de.pdf**

Die Anleitung zu ersten Schritten enthält detaillierte Informationen zur Installation, Einrichtung und Prüfung von GFI EndPointSecurity.

## 1.4 Lizenzierung von GFI EndPointSecurity

Weitere Informationen zur Lizenzierung und Testversion, finden Sie auf der GFI-Website unter:

**http://www.gfi.com/products/gfi-endpointsecurity/pricing/licensing**

# 2 Informationen zu GFI EndPointSecurity

## 2.1 Einführung

In diesem Kapitel werden folgende Themen behandelt:

» Hauptfunktionen und -komponenten von GFI EndPointSecurity

» Funktionsweise von GFI EndPointSecurity

» Von GFI EndPointSecurity unterstützte Gerätekategorien und Schnittstellen

## 2.2 Hauptfunktionen

GFI EndPointSecurity beinhaltet folgende Hauptfunktionen:

### *Gruppenbasierter Zugriffsschutz*

GFI EndPointSecurity erlaubt es Ihnen, Computer in Gruppen einzuteilen, für die eigene Schutzrichtlinien definiert sind. Richtlinieneinstellungen gelten übergreifend für alle Mitglieder einer Gruppe.

### *Differenzierte Zugriffskontrolle*

Sie können ausgewählten Netzwerkbenutzern den Zugriff auf ein bestimmtes Einzelgerät erlauben oder untersagen. Erteilen Sie zudem für alle freigegebenen Geräte (z. B. CV/DVD-Laufwerke, PDAs) je nach Benutzer lediglich Lese- oder auch Vollzugriffsrechte.

### *Bereitstellung von Richtlinien nach Zeitplan*

GFI EndPointSecurity ermöglicht die Planung der Bereitstellung von Schutzrichtlinien und die Änderung verwandter Konfigurationen, ohne dass die GFI EndPointSecurity-Verwaltungskonsole geöffnet werden muss. Die Bereitstellungsfunktion steuert auch fehlgeschlagene Bereitstellungen durch eine automatische Neuplanung.

### *Zugriffssteuerung*

GFI EndPointSecurity erlaubt es Ihnen, den Zugriff nicht nur unter Berücksichtigung einzelner Gerätekategorien zu sperren, sondern auch über:

» Dateityp – Benutzer dürfen beispielsweise Dateien im doc-Format öffnen, exe-Dateien sind jedoch gesperrt.

» Physische Schnittstelle – Alle Geräte, die über physische Schnittstellen wie USB angeschlossen sind.

» Gerätekennung – Unter Berücksichtigung der eindeutigen Hardware-ID kann der Zugriff für ein einzelnes Gerät unterbunden werden.



Unter Microsoft Windows 7 kann die Funktion **BitLocker To Go** verwendet werden, um Daten auf Wechseldatenträgern zu verschlüsseln und zu schützen. GFI EndPointSecurity überprüft gültige Dateitypen, die mit BitLocker To Go von Windows 7 verschlüsselt wurden.

### *Geräte-Whitelist und -Blacklist*

Administratoren können einzelne Geräte, die stets oder nie zugänglich sein dürfen, auf eine Whitelist bzw. Blacklist setzen.

### *Hauptbenutzer*

Administratoren können Benutzer oder Gruppen festlegen, die auf Geräte, die ansonsten durch GFI EndPointSecurity blockiert sind, stets Vollzugriff haben.

### *Zeitlich begrenzter Zugriff*

Administratoren haben die Möglichkeit, auf einem bestimmten Computer den Zugriff auf ein tragbares Gerät oder eine Gerätegruppe zeitlich begrenzt zu gestatten. Mithilfe eines speziell erstellten Entsperrcodes kann ein Mitarbeiter mit dieser Funktion somit innerhalb einer festgelegten Frist ein für seinen Computer zuvor gesperrtes Gerät oder eine Schnittstelle nutzen, selbst wenn der Agent von GFI EndPointSecurity keine Verbindung mit dem Netzwerk hält.

### *Statusanzeige*

Die Benutzeroberfläche des Dashboards zeigt den Status von bereitgestellten Agenten zum Zugriffsschutz, der Datenbank und Warnservern, des GFI EndPointSecurity-Dienstes sowie grafisch aufbereitete statistische Daten an.

Der aktuelle Status sämtlicher bereitgestellter Agenten zum Zugriffsschutz wird von der Hauptanwendung kontinuierlich überprüft. Wartungsaufgaben werden automatisch durchgeführt, sobald ein Agent online ist.

### *Active Directory-Bereitstellung per MSI*

Über die GFI EndPointSecurity-Verwaltungskonsole lässt sich eine MSI-Datei erstellen, die später mithilfe der Active Directory-Funktion für Gruppenrichtlinienobjekte oder mithilfe anderer Bereitstellungsoptionen bereitgestellt werden kann. Eine MSI-Datei umfasst alle in einer einzelnen Schutzrichtlinie festgelegten Sicherheitseinstellungen.

### *Kennwortgeschützte Verwaltung von Agenten*

Funktionen zur Verwaltung von Agenten (z. B. zur Aktualisierung oder Deinstallation) sind über ein individuell festlegbares Kennwort geschützt. Andere Instanzen von GFI EndPointSecurity können agentenspezifische Verwaltungsoptionen somit nicht aufrufen.

### *Gerätesuche*

Die GFI EndPointSecurity-Engine dient dem Scannen und Erkennen von mobilen Geräten im Netzwerk, selbst auf Computern, die keiner Schutzrichtlinie zugewiesen sind. Unter Verwendung der gewonnenen Daten über erkannte Geräte lassen sich für einzelne Geräte Sicherheitsrichtlinien erstellen und Zugriffsrechte zuweisen.

### *Protokoll-Browser*

Administratoren können mit dem integrierten Tool die von GFI EndPointSecurity im Datenbank-Backend aufgezeichneten Protokolle zur Benutzeraktivität und Geräteverwendung anzeigen.

### *Ausgabe von Warnungen*

GFI EndPointSecurity ermöglicht bei Anschluss/Trennung oder Sperrung/Freigabe eines Geräts sowie bei dienstegenerierten Ereignissen E-Mail-Warnungen sowie Netzwerk- und SMS-Nachrichten zu konfigurieren und an bestimmte Empfänger zu senden.

### *Anpassbare Popup-Meldungen*

Wird Benutzern beispielsweise der Zugang zu einem Gerät verwehrt, werden sie durch eine Popup-Meldung über die Sperrung informiert. GFI EndPointSecurity ermöglicht die Anpassungen dieser Meldungen.

### *Datenbankwartung*

Zur Kontrolle der Größe des Datenbank-Backends kann GFI EndPointSecurity so konfiguriert werden, dass Ereignisse, die älter als ein festgelegter Zeitraum sind, gesichert oder gelöscht werden.

## 2.3 Programmkomponenten von GFI EndPointSecurity

Bei der Installation von GFI EndPointSecurity werden folgende Komponenten eingerichtet:

- GFI EndPointSecurity-Verwaltungskonsole
- GFI EndPointSecurity-Agent.

*GFI EndPointSecurity-Verwaltungskonsole*

Durch Navigieren in der GFI EndPointSecurity-Verwaltungskonsole können Sie:

- Schutzrichtlinien erstellen und verwalten, und festlegen, welche Gerätekategorien und Schnittstellen kontrolliert werden sollen.
- Schutzrichtlinien und Agenten per Fernzugriff auf den zu kontrollierenden Computern bereitstellen sowie zeitlich begrenzten Zugriff auf Computer gewähren, um bestimmte Geräte zu nutzen.
- Den Schutzstatus jedes kontrollierten Computers anzeigen.
- Überwachte Computer scannen, um aktuell oder zuvor verbundene Geräte zu identifizieren.
- Protokolle prüfen, und analysieren, welche Geräte mit den einzelnen Netzwerkcomputern verbunden waren.
- Verfolgen, auf welchen Computern der Agent bereitgestellt wurde und welche Agenten aktualisiert werden müssen.

*Der GFI EndPointSecurity-Agent*

Der Agent von GFI EndPointSecurity sorgt dafür, dass die Schutzrichtlinien auf den zu kontrollierenden Computern eingerichtet werden. Dieser Dienst wird automatisch auf dem zu kontrollierenden Netzwerkcomputer installiert, nachdem die erste relevante Schutzrichtlinie von der GFI EndPointSecurity-Verwaltungskonsole bereitgestellt wurde. Bei weiteren Bereitstellungen der gleichen Schutzrichtlinie wird der Agent aktualisiert, nicht neu installiert.

## 2.4 Funktionsweise von GFI EndPointSecurity – Bereitstellung und Überwachung

Die Bereitstellung von Schutzrichtlinien und die Überwachung durch GFI EndPointSecurity erfolgt in vier Phasen:

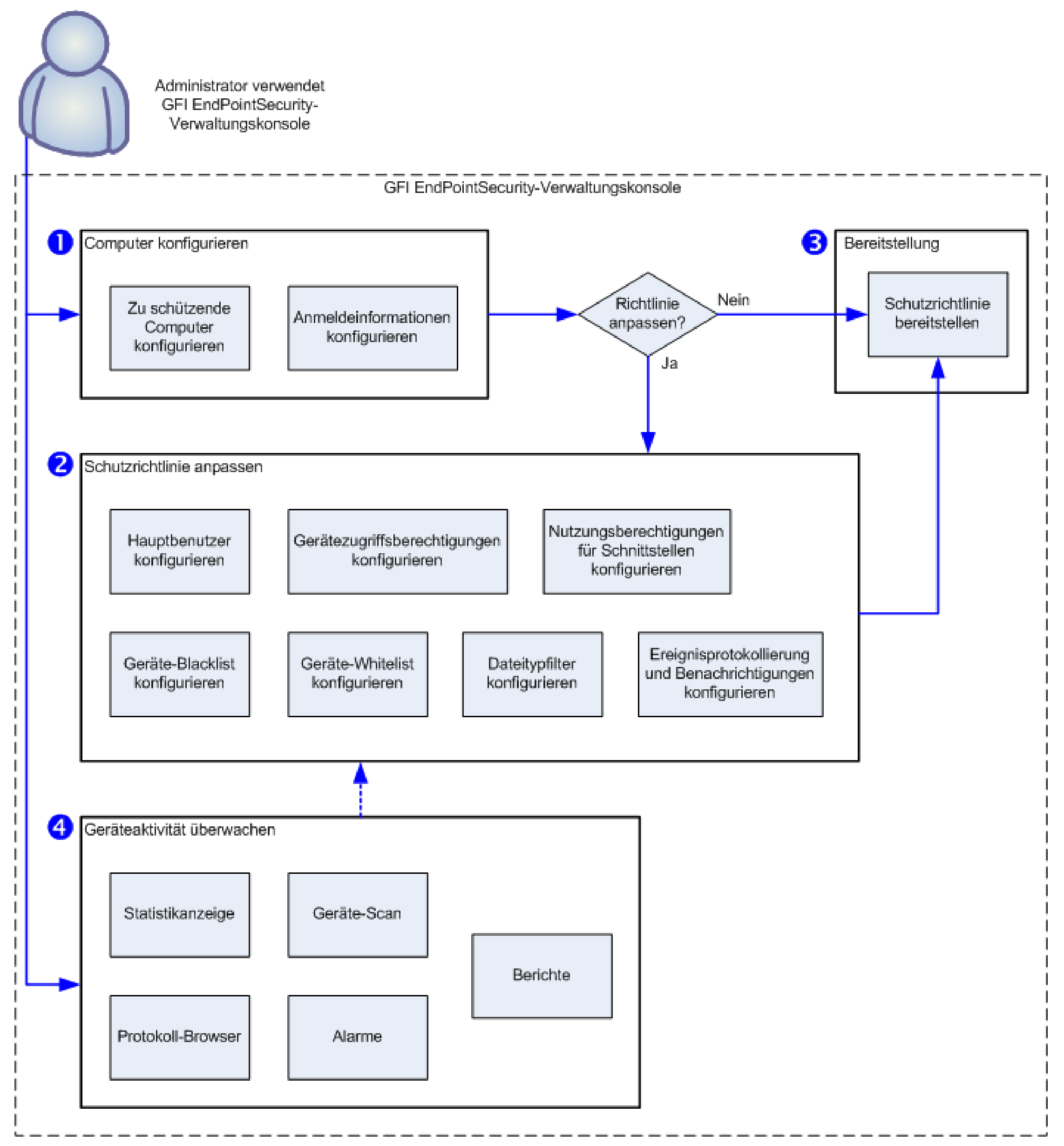



*Abbildung 1 - Bereitstellung einer Schutzrichtlinie und Überwachung*

**Phase 1 – Konfigurieren von Computern** Der Administrator muss festlegen, welche Schutzrichtlinie welchen Computern zugewiesen wird. Zudem sind die von GFI EndPointSecurity zu verwendenden Anmeldeinformationen anzugeben, die für den Zugriff auf zu kontrollierenden Computer und die Bereitstellung des Agenten erforderlich sind.

**Phase 2 – Anpassen von Schutzrichtlinien:** Vor oder nach der Bereitstellung einer Schutzrichtlinie kann diese vom Administrator angepasst werden. Beispielsweise können Hauptbenutzer angegeben, Geräte auf die Blacklist/Whitelist gesetzt und Zugriffsberechtigungen für Geräte definiert werden.

**Phase 3 - Bereitstellen von Schutzrichtlinien:** Der Administrator stellt die Schutzrichtlinie bereit. Bei der ersten Bereitstellung einer Schutzrichtlinie wird automatisch ein GFI EndPointSecurity-Agent auf dem zu kontrollierenden Netzwerkcomputer installiert. Bei weiteren Bereitstellungen der gleichen Schutzrichtlinie wird der Agent aktualisiert, nicht neu installiert.

**Phase 4 – Überwachen des Gerätezugriffs:** Ist der Agent auf den zu kontrollierenden Computern bereitgestellt, kann der Administrator alle Zugriffsversuche auf Geräte über die GFI EndPointSecurity-Verwaltungskonsole überwachen sowie Alarmmeldungen und Berichte über GFI EndPointSecurity ReportPack empfangen und generieren.

## 2.5 Funktionsweise von GFI EndPointSecurity - Gerätezugriff

Der mit GFI EndPointSecurity kontrollierte und gesteuerte Gerätezugriff erfolgt in drei Phasen:

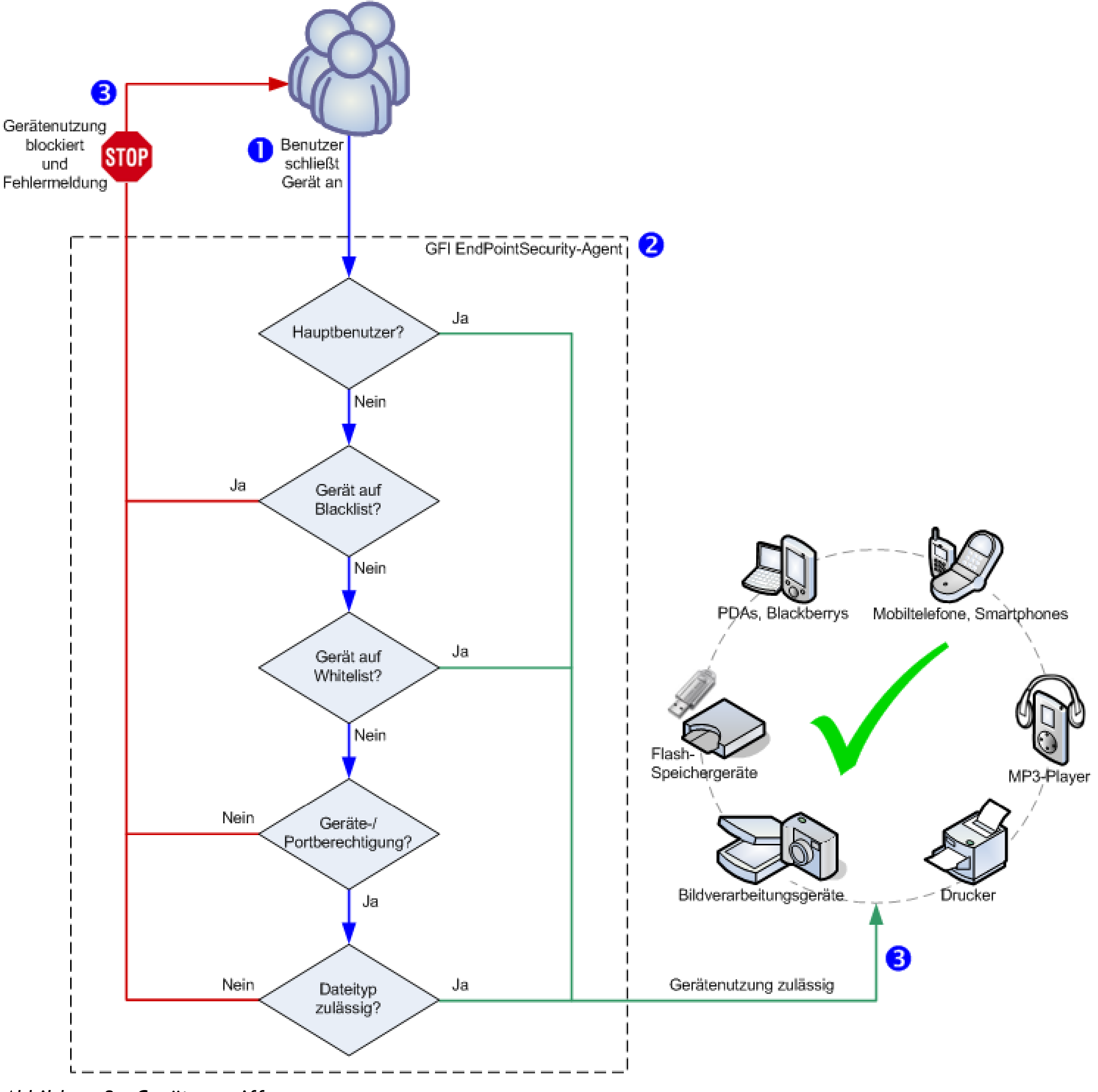



*Abbildung 2 - Gerätezugriff*

**Phase 1 - Anschließen eines Geräts an einen kontrollierten Computer:** Ein Benutzer schließt ein Gerät an einen durch GFI EndPointSecurity kontrollierten Computer an.

**Phase 2 - Durchsetzen von Schutzrichtlinien:** Der auf dem kontrollierten Computer installierte Agent für den Zugriffsschutz erkennt das angeschlossene Gerät und überprüft die für den Computer/Benutzer anzuwendenden Schutzrichtlinien. Dieser Vorgang bestimmt, ob der Zugriff auf das Gerät zugelassen oder blockiert wird.

**Phase 3 - Freigeben/Sperren der Verwendung eines Geräts:** Je nach Ergebnis der Prüfung aus Phase 2 erhält der Benutzer entweder eine Meldung, dass ein Zugriff auf das angeschlossene Gerät untersagt wurde, oder der Zugriff wird zugelassen.

## 2.6 Funktionsweise von GFI EndPointSecurity - Zeitlich begrenzter Zugriff

Der durch GFI EndPointSecurity zeitlich begrenzte Gerätezugriff erfolgt in drei Phasen:

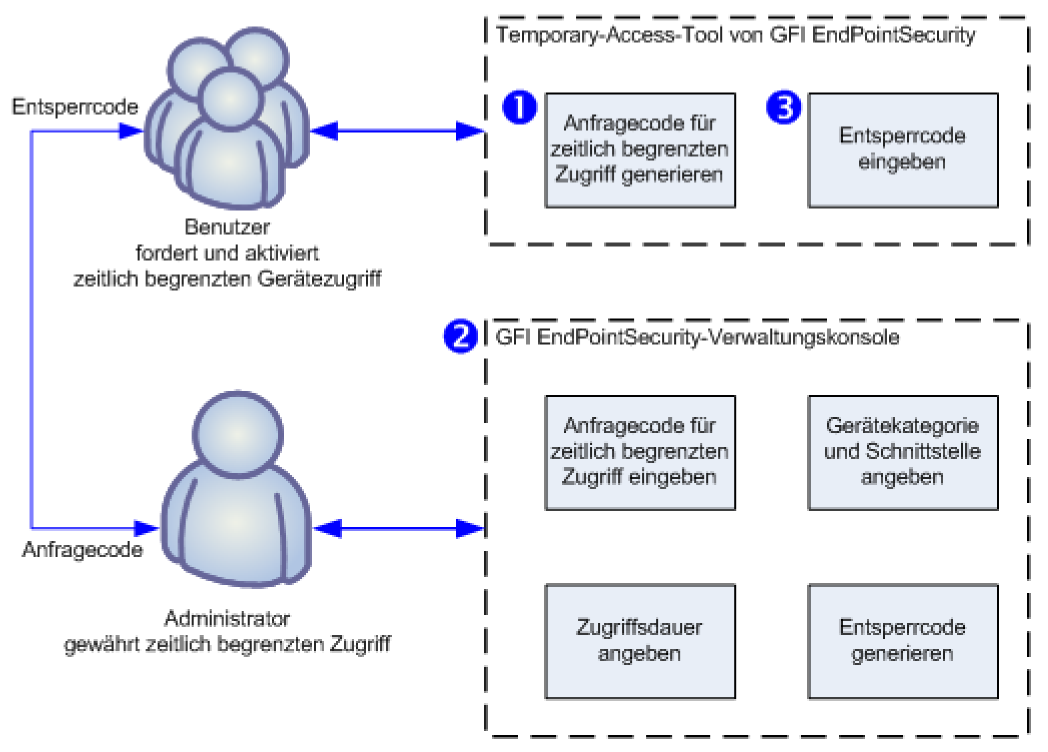



*Abbildung 3 - Anfordern/Zulassen eines zeitlich begrenzten Zugriffs*

**Phase 1 - Benutzeranfrage für zeitlich begrenzten Gerätezugriff:** Soll auf ein an einen Computer angeschlossenes Gerät zugegriffen werden, startet der Benutzer dort das Temporary-Access-Tool von GFI EndPointSecurity. Mit diesem Tool wird eine Anfrage mit Anfragecode für den zeitlich begrenzten Gerätezugriff an den Administrator übermittelt. Der Benutzer muss neben der Dauer des gewünschten Zugriffs auch die Gerätekategorie oder die Schnittstelle angeben, auf die zugegriffen wird.

**Phase 2 - Freigabe des zeitlich begrenzten Gerätezugriffs:** Der Administrator verwendet die Funktion für den zeitlich begrenzten Zugriff der GFI EndPointSecurity-Verwaltungskonsole, um den Anfragecode einzugeben sowie die Geräte/Schnittstellen und die Zugriffsdauer festzulegen. Daraufhin wird ein Entsperrcode erstellt und zur vorübergehenden Freischaltung des Geräts an den Benutzer übermittelt. Der Code ist abschließend vom Benutzer im Temporary-Access-Tool einzugeben.

**Phase 3 - Benutzer aktiviert zeitlich begrenzten Gerätezugriff:** Sobald der Benutzer den Entsperrcode vom Administrator erhält, muss dieser im Temporary-Access-Tool von GFI EndPointSecurity eingegeben werden, um den zeitlich begrenzten Zugriff zu aktivieren und die erforderlichen Geräte/Schnittstellen nutzen zu können.

## 2.7 Unterstützte Gerätekategorien

GFI EndPointSecurity unterteilt kontrollierte Hardware in folgende Gerätekategorien:

- Disketten
- CD/DVD
- Speichergeräte
    - USB-Speichersticks
    - Multimedia-Player (z. B. MP3-/MP4-Player)
    - Kartenleser für CompactFlash- und andere Speicherkarten
    - USB-Multi-Drives (d. h. Geräte, die nicht als einzelnes Laufwerk angeschlossen werden)
    - Weitere tragbare Speichermedien

- Drucker
- PDAs
  - Pocket-PCs
  - Smartphones
- Netzwerkadapter
  - WLAN
  - Wechselnetzwerkadapter (z. B. USB, FireWire, PCMCIA)
- Modems
  - Smartphones
  - Mobiltelefone
- Bildverarbeitungsgeräte
  - Digitalkameras
  - Webcams
  - Scanner
- Eingabegeräte
  - Tastaturen
  - Mäuse
  - Spiel-Controller
- Weitere Geräte
  - Bluetooth-Dongles/Schnittstellen
  - Infrarot-Dongles/Schnittstellen
  - MO-Laufwerke (intern und extern)
  - Zip-Laufwerke
  - Bandlaufwerke.

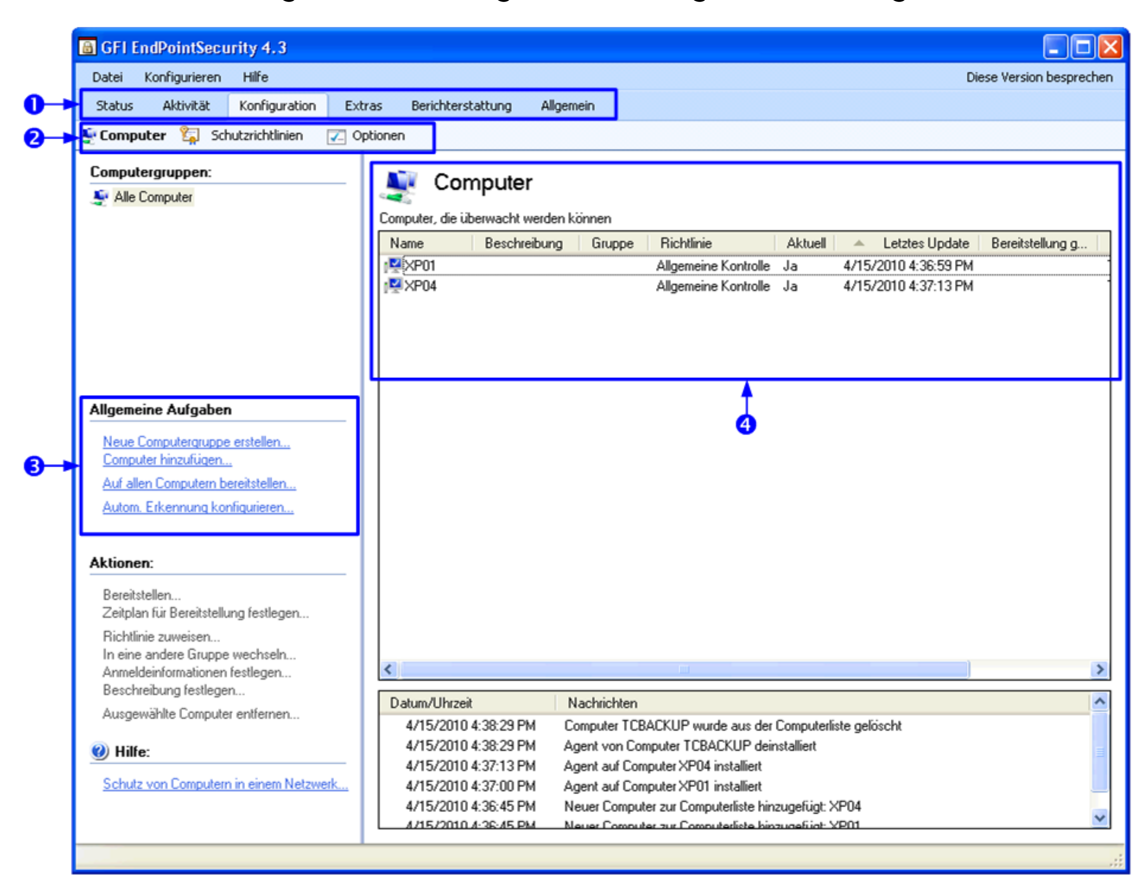
## 2.8 Unterstützte Geräteschnittstellen

GFI EndPointSecurity sucht nach Geräten, die an folgenden Schnittstellen angeschlossen sind oder waren:

- USB
- FireWire
- PCMCIA
- Bluetooth
- Serielle und parallele Ports
- Infrarot
- Secure Digital (SD)
- Interne (z. B. optische und Diskettenlaufwerke)

## 2.9 Navigieren in der GFI EndPointSecurity-Verwaltungskonsole

Die GFI EndPointSecurity-Verwaltungskonsole enthält alle administrativen Funktionen, die für die Überwachung und Verwaltung des Gerätezugriffs notwendig sind.




*Screenshot 1 - GFI EndPointSecurity: Verwaltungskonsole*

**1** **Registerkarten** – Ermöglicht die Navigation zwischen den verschiedenen Registerkarten der GFI EndPointSecurity-Verwaltungskonsole. Die verfügbaren Registerkarten sind:

- » **Status** – Ermöglicht die Überwachung des Programmstatus von GFI EndPointSecurity und von statistischen Zugriffsdaten.
- » **Aktivität** – Ermöglicht die Überwachung der im Netzwerk verwendeten Geräte.
- » **Konfiguration** – Ermöglicht den Aufruf und die Anpassung der standardmäßigen Schutzrichtlinien.
- » **Extras** – Ermöglicht den Scan von kontrollierten Computern zur Erkennung von angeschlossenen Geräten.
- » **Berichterstellung** – Ermöglicht die Anzeige von Informationen zu GFI EndPointSecurity ReportPack.
- » **Allgemein** – Ermöglicht die Prüfung auf GFI EndPointSecurity-Aktualisierungen sowie die Anzeige der Version und Lizenzierungsdetails.

**2** **Untergeordnete Registerkarten** – Ermöglicht den Zugriff auf weitere Informationen und Einstellungen innerhalb der GFI EndPointSecurity-Verwaltungskonsole.

**3** **Linker Bereich** – Ermöglicht die Auswahl zusätzlicher Konfigurationsoptionen für GFI EndPointSecurity. Die Konfigurationsoptionen sind in verschiedene Gruppen eingeteilt: **Allgemeine Aufgaben**, **Aktionen** und **Hilfe.** Nur bei manchen Registerkarten verfügbar.

4 **Rechter Bereich** – Ermöglicht die Konfiguration der Konfigurationsoptionen, die im linken Bereich ausgewählt wurden. Nur bei manchen Registerkarten verfügbar.

# 3 Erstellen neuer Schutzrichtlinien

## 3.1 Einführung

GFI EndPointSecurity wird mit einer Standardschutzrichtlinie geliefert, so dass die Software nach der Installation sofort betriebsbereit ist. Sie können anschließend weitere Schutzrichtlinien erstellen, um den Gerätezugriff unternehmensspezifisch anzupassen. In diesem Kapitel finden Sie Informationen zur Erstellung neuer Schutzrichtlinien mithilfe des Assistenten zur Erstellung von Schutzrichtlinien.

Der Assistent zur Erstellung von Schutzrichtlinien führt Sie für jede Schutzrichtlinie durch die Konfiguration folgender Einstellungen:

- Richtlinienname
- Erstellung einer Einstellungsvererbung
- Überwachte Gerätekategorien
- Überwachte Schnittstellen
- Globale Berechtigungen
- Dateityp-Filter
- Verschlüsselungsberechtigungen
- Protokollierungsoptionen
- Warnoptionen.

## 3.2 Assistent zur Erstellung von Schutzrichtlinien

Verwenden Sie den Assistenten zur Erstellung von neuen Schutzrichtlinien, um neue Richtlinien zu erstellen:

### *Schritt 1: Starten des Assistenten zur Erstellung von Schutzrichtlinien*

So starten Sie den Assistenten zur Erstellung von Schutzrichtlinien:

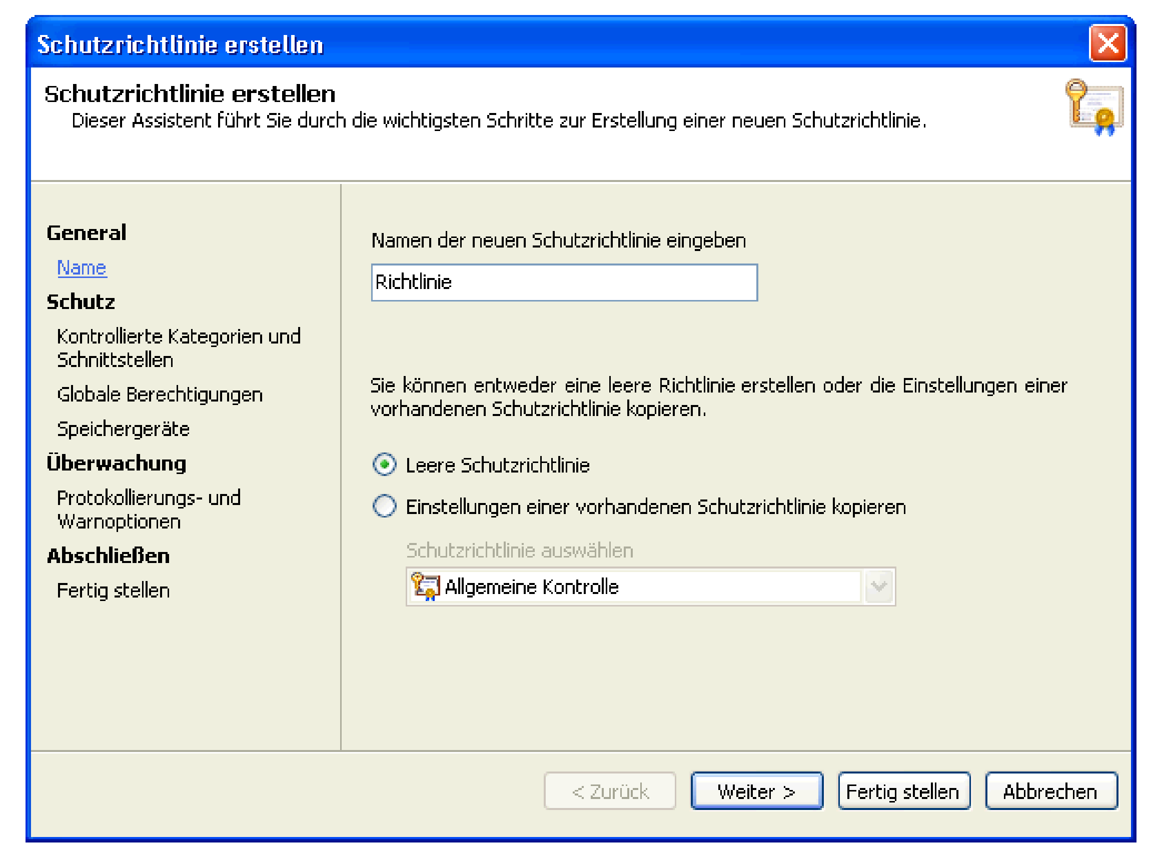
1. Klicken Sie in der GFI EndPointSecurity-Verwaltungskonsole auf die Registerkarte **Konfiguration**.

2. Klicken Sie auf die untergeordnete Registerkarte **Schutzrichtlinien**.

3. Klicken Sie im linken Bereich im Abschnitt **Allgemeine Aufgaben** auf den Hyperlink **Neue Schutzrichtlinie erstellen...**.

### *Schritt 2: Konfigurieren des Richtliniennamens und Erstellen einer Einstellungsvererbung*

GFI EndPointSecurity bietet Ihnen die Möglichkeit, neue Schutzrichtlinien zu erstellen und jede Schutzrichtlinie mit neuen Einstellungen zu konfigurieren oder die Einstellungen einer vorhandenen Schutzrichtlinie zu vererben.




*Screenshot 2 - Assistent zur Erstellung von Schutzrichtlinien von GFI EndPointSecurity: Namensgebung*

So konfigurieren Sie den Richtlinienname und erstellen eine Einstellungsvererbung für diese Schutzrichtlinie:

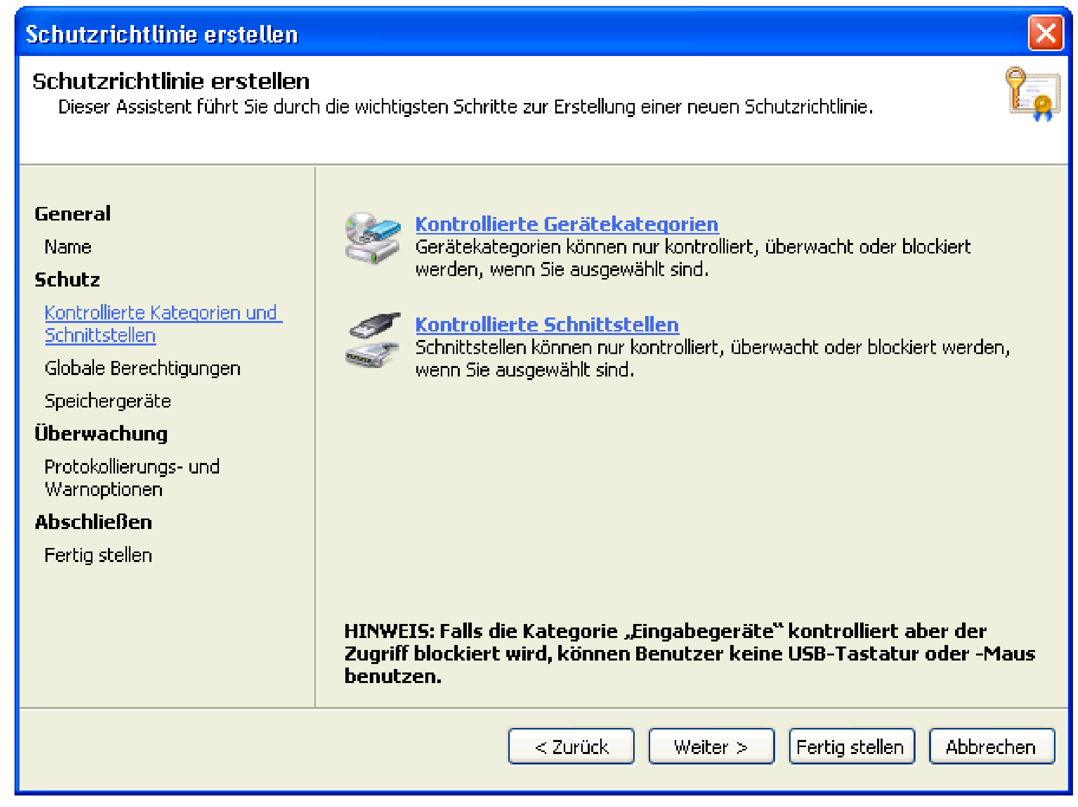
1. Geben Sie einen Namen für die neue Schutzrichtlinie ein.
2. Wählen Sie im Einstellungsbereich die erforderliche Vererbungsoption aus:
   - **Leere Schutzrichtlinie** – Zur Erstellung einer neuen Schutzrichtlinie mit benutzerdefinierten Einstellungen.
   - **Einstellungen einer vorhandenen Schutzrichtlinie kopieren** – Zur Vererbung der Einstellungen einer vorhandenen Schutzrichtlinie. Wählen Sie aus dem Dropdown-Menü die Schutzrichtlinie, von der die Einstellungen vererbt werden sollen. Der Assistent führt Sie direkt zur Seite der Richtlinien. Prüfen Sie die Seite der Richtlinien, und klicken Sie auf **Fertigstellen**, um den Assistenten zu beenden.
3. Klicken Sie auf **Weiter**.

### *Schritt 3: Konfigurieren kontrollierter Kategorien und Schnittstellen*

GFI EndPointSecurity bietet Ihnen die Möglichkeit, festzulegen, welche Gerätekategorien und Schnittstellen durch die Schutzrichtlinie kontrolliert, überwacht und blockiert werden sollen.



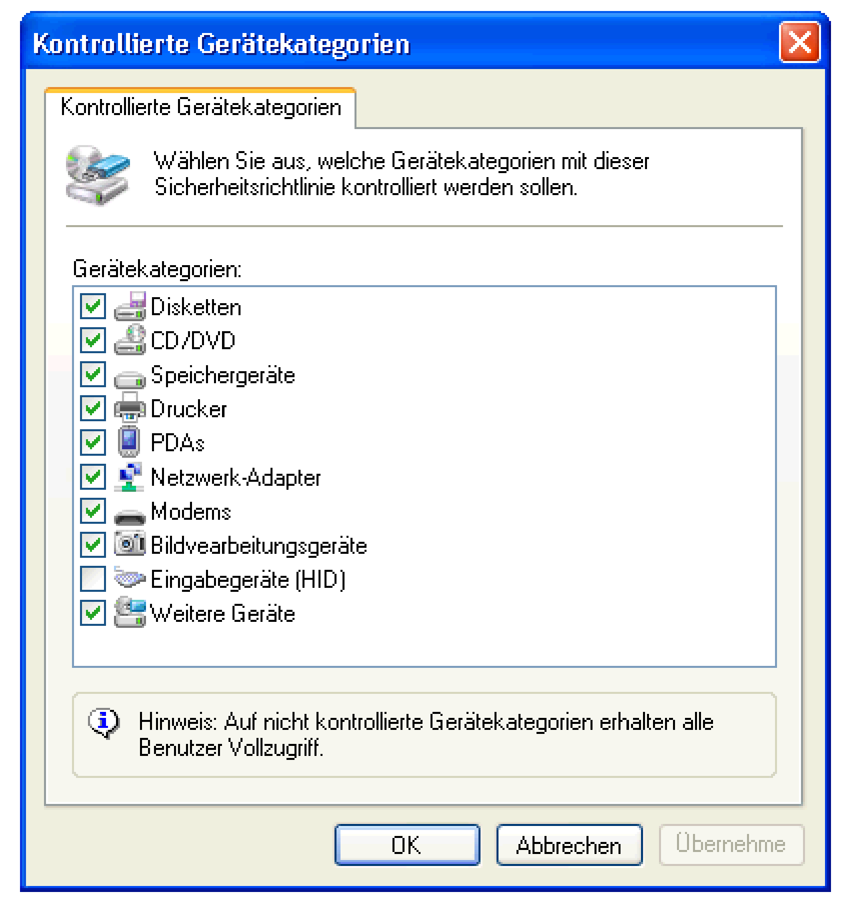
Nicht festgelegte Geräte und Schnittstellen sind über die von der Schutzrichtlinie kontrollierten Computer uneingeschränkt zugänglich.




*Screenshot 3 - Assistent zur Erstellung von Schutzrichtlinien von GFI EndPointSecurity: Kontrollierte Kategorien und Schnittstellen*

So geben Sie die Geräte und Schnittstellen an, die durch diese Schutzrichtlinie kontrolliert werden sollen:

1. Klicken Sie auf den Hyperlink **Kontrollierte Gerätekategorien**.



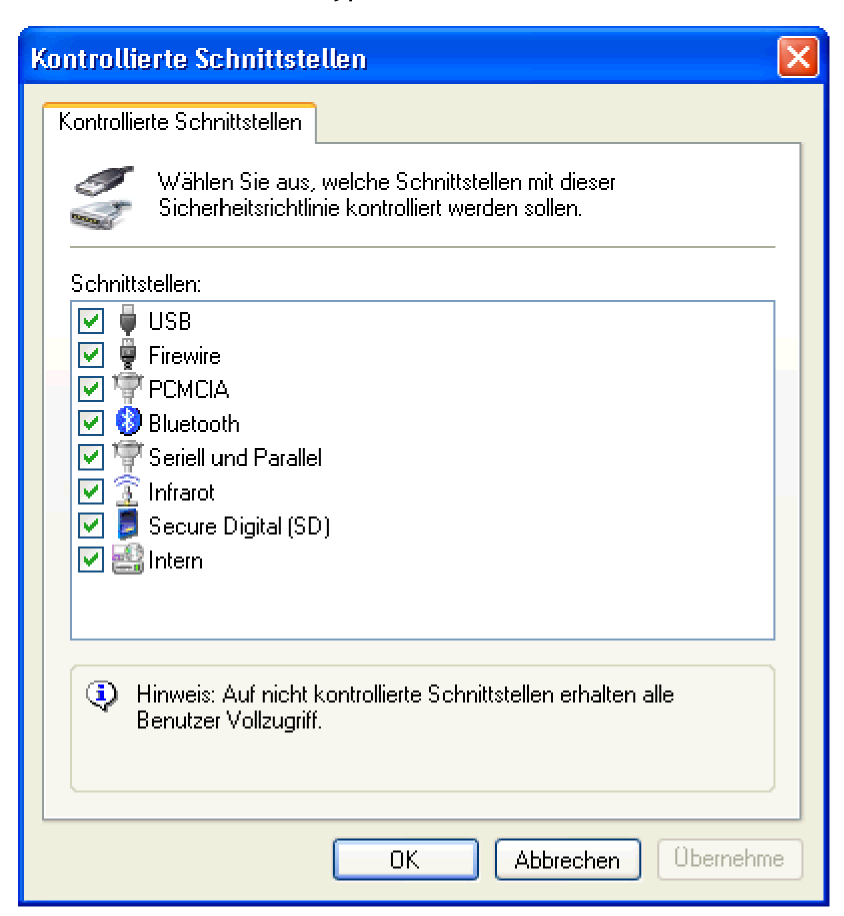

*Screenshot 4 - Optionen für kontrollierte Gerätekategorien*

2. Aktivieren bzw. deaktivieren Sie im Dialog **Kontrollierte Gerätekategorien** die erforderlichen Gerätekategorien, die durch die Schutzrichtlinie kontrolliert werden sollen. Klicken Sie anschließend auf **OK**.



Falls die Option **Eingabegeräte** aktiviert ist und der Zugriff verweigert wird, können Benutzer keine USB-Tastaturen oder -Mäuse verwenden, die an die durch diese Schutzrichtlinie kontrollierten Computer angeschlossen sind.

3. Klicken Sie auf den Hyperlink **Kontrollierte Schnittstellen**.




*Screenshot 5 - Optionen für kontrollierte Schnittstellen*

4. Aktivieren bzw. deaktivieren Sie im Dialog **Kontrollierte Schnittstellen** die erforderlichen Schnittstellen, die durch die Schutzrichtlinie kontrolliert werden sollen. Klicken Sie anschließend auf **OK**.

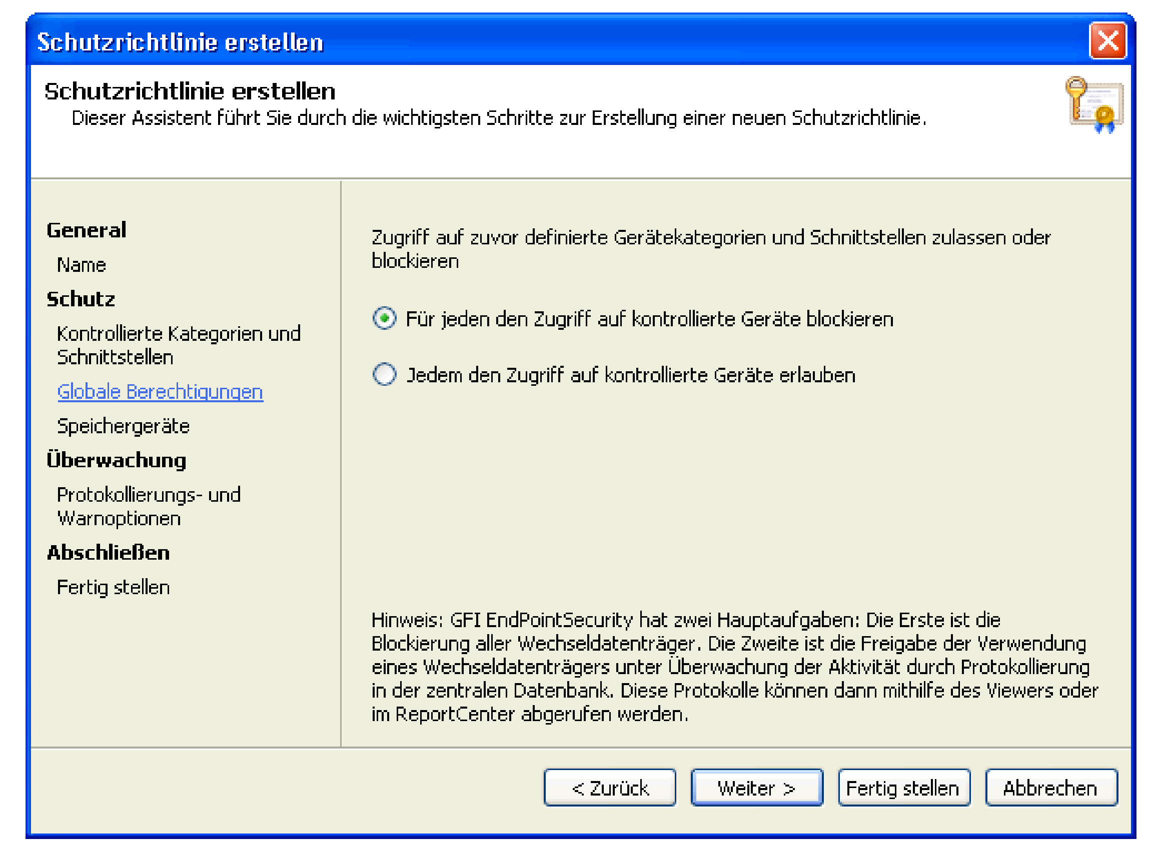
5. Klicken Sie auf **Weiter**.

### *Schritt 4: Konfigurieren globaler Berechtigungen*

GFI EndPointSecurity bietet Ihnen die Möglichkeit, alle Geräte einer Kategorie oder Geräte an bestimmten Schnittstellen, die im vorherigen Schritt ausgewählt wurden, zu blockieren oder zugänglich zu machen.



Der Zugriff kann später für bestimmte Geräte, Benutzer oder kontrollierte Computer blockiert bzw. zugelassen werden. Weitere Informationen finden Sie im Kapitel Anpassen von Schutzrichtlinien in diesem Handbuch.




*Screenshot 6 - Assistent zur Erstellung von Schutzrichtlinien von GFI EndPointSecurity: Globale Berechtigungen*

So konfigurieren Sie globale Zugriffsberechtigungen für diese Schutzrichtlinie:

1. Wählen Sie im Berechtigungsbereich die erforderlichen globalen Zugriffsberechtigungen aus:

   » **Für jeden den Zugriff auf kontrollierte Geräte blockieren** – Zur Blockierung des Zugriffs auf alle ausgewählten Geräte/Schnittstellen.

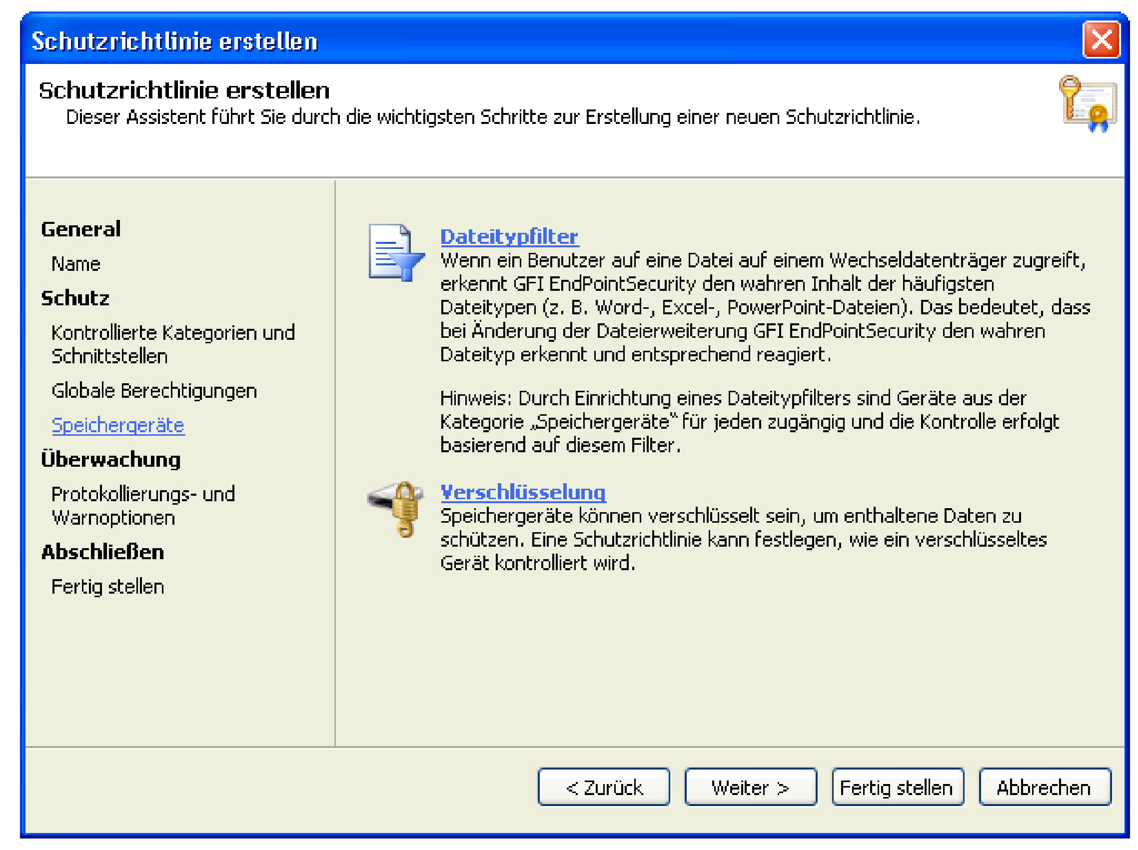
   » **Jedem den Zugriff auf kontrollierte Geräte erlauben** – Zur Zulassung des Zugriffs auf alle ausgewählten Geräte/Schnittstellen. Falls Sie diese Option auswählen, erfolgt dennoch eine Aktivitätsüberwachung auf allen durch dieses Schutzrichtlinie kontrollierten Computern.

2. Klicken Sie auf **Weiter**.

### *Schritt 5: Konfigurieren der Speichergeräte*

GFI EndPointSecurity bietet die Möglichkeit, den Zugriff basierend auf Dateitypen einzuschränken. Außerdem kann der wahre Inhalt der meisten Dateitypen (z. B. .doc oder .xls) erkannt werden. Dadurch können die für den Dateityp erforderlichen Maßnahmen ergriffen werden. Das ist besonders nützlich, wenn Dateierweiterungen böswillig manipuliert werden.

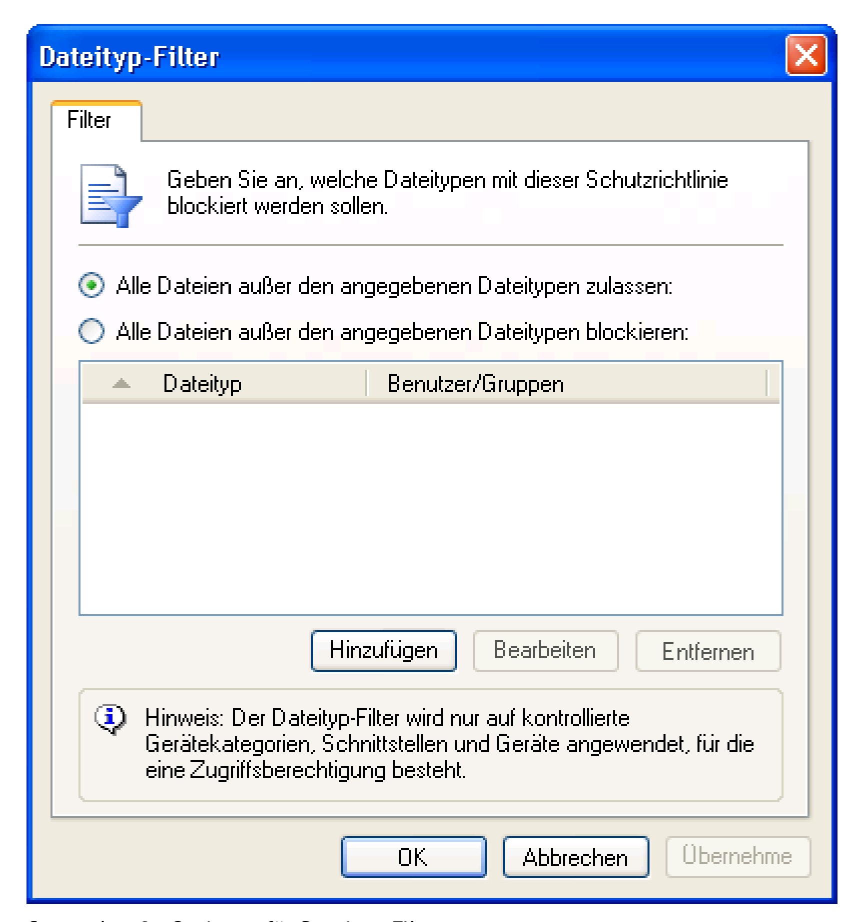
Zusätzlich können Sie für Active Directory (AD)-Benutzer und/oder -Benutzergruppen, oder für lokale Benutzer und/oder Benutzerschemen den Zugriff auf bestimmte Dateitypen auf Geräten, die mit BitLocker To Go (einer Funktion von Microsoft Windows 7) verschlüsselt wurden, einschränken. Diese Einschränkungen werden angewendet, wenn verschlüsselte Geräte an die durch die Schutzrichtlinie kontrollierten Computer angeschlossen werden.




*Screenshot 7 - Assistent zur Erstellung von Schutzrichtlinien von GFI EndPointSecurity: Speichergeräte*

So konfigurieren Sie Einschränkungen basierend auf dem Dateityp und Einschränkungen für Geräte, die für diese Schutzrichtlinie mit BitLocker To Go verschlüsselt wurden:

1. Klicken Sie auf den Hyperlink **Dateityp-Filter**.

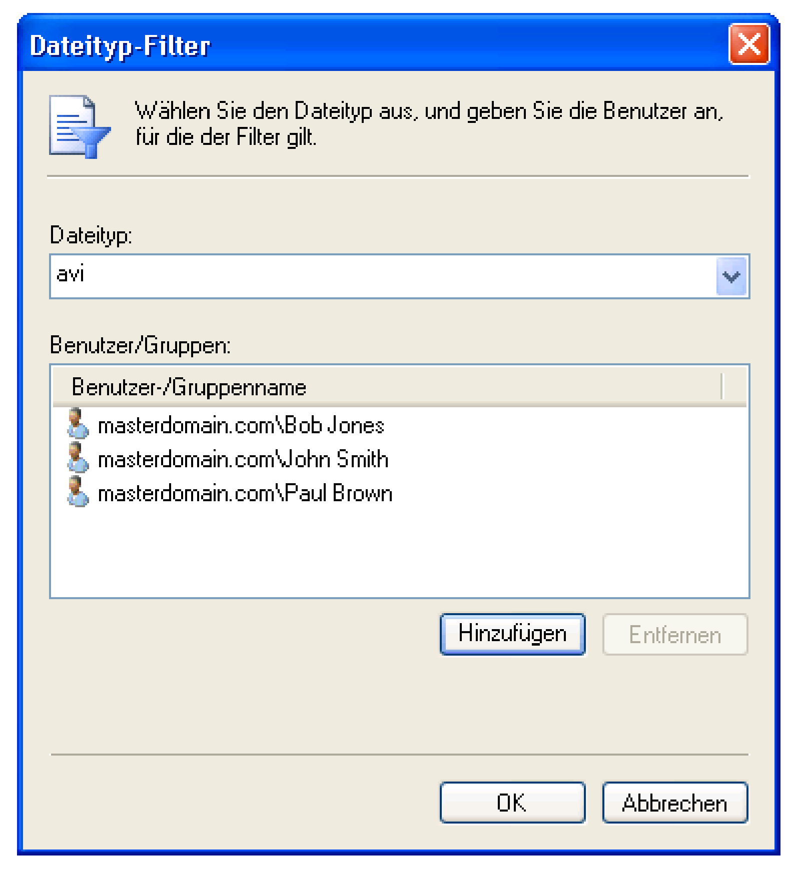



*Screenshot 8 - Optionen für Dateityp-Filter*

2. Wählen Sie im Dialog **Dateityp-Filter** die auf diese Schutzrichtlinie anzuwendende Einschränkung aus:

» Alle Dateien außer den angegebenen Dateitypen zulassen

» Alle Dateien außer den angegebenen Dateitypen blockieren




*Screenshot 9 - Optionen für Dateityp-Filter und Benutzer*

3. Klicken Sie auf **Hinzufügen…**, und wählen Sie den Dateityp aus dem Dropdown-Menü **Dateityp** aus oder geben Sie ihn ein.

4. Klicken Sie auf **Hinzufügen...**, um die Benutzer/Gruppen festzulegen, die auf diesen Dateityp zugreifen können oder dafür gesperrt sind. Klicken Sie anschließend auf **OK**.

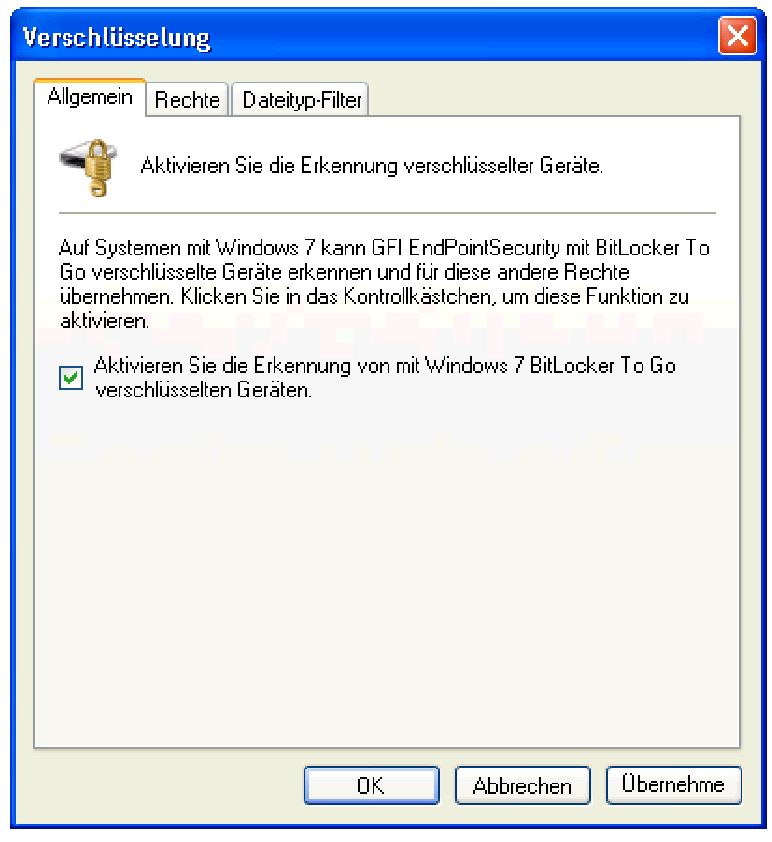
Wiederholen Sie die vorherigen 2 Unterschritte für jeden zu beschränkenden Dateityp.

5. Klicken Sie zweimal auf **OK**.



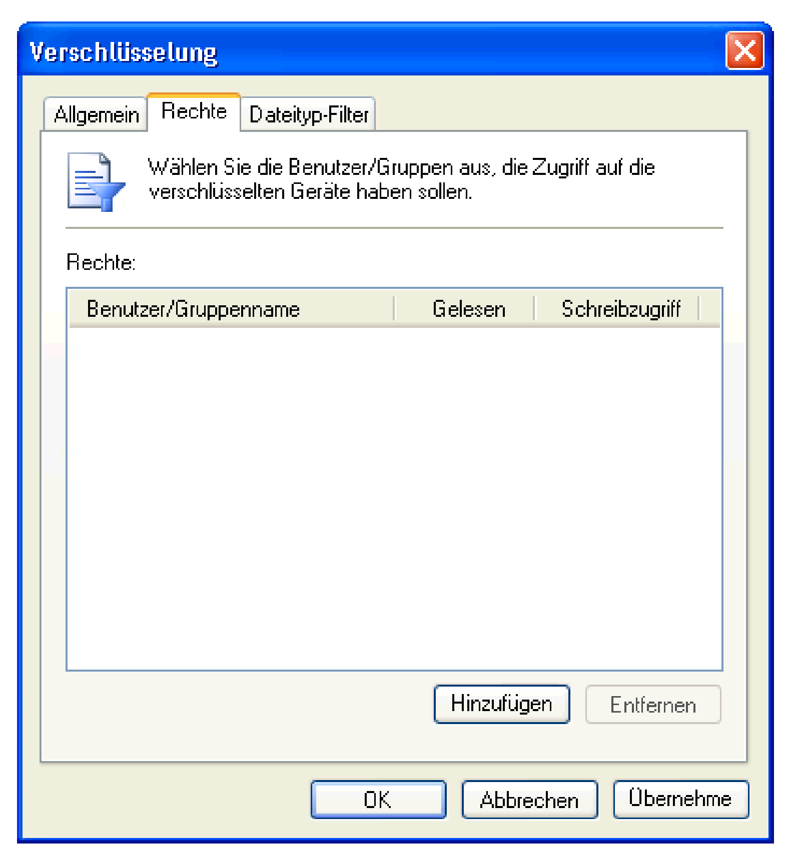
Weitere Informationen zu Dateitypüberprüfungen finden Sie im Kapitel Anpassen von Schutzrichtlinien unter Konfigurieren der Dateitypfilter.

6. Klicken Sie auf den Hyperlink **Verschlüsselung**.




*Screenshot 10 - Verschlüsselungsoptionen - Registerkarte „Allgemein"*

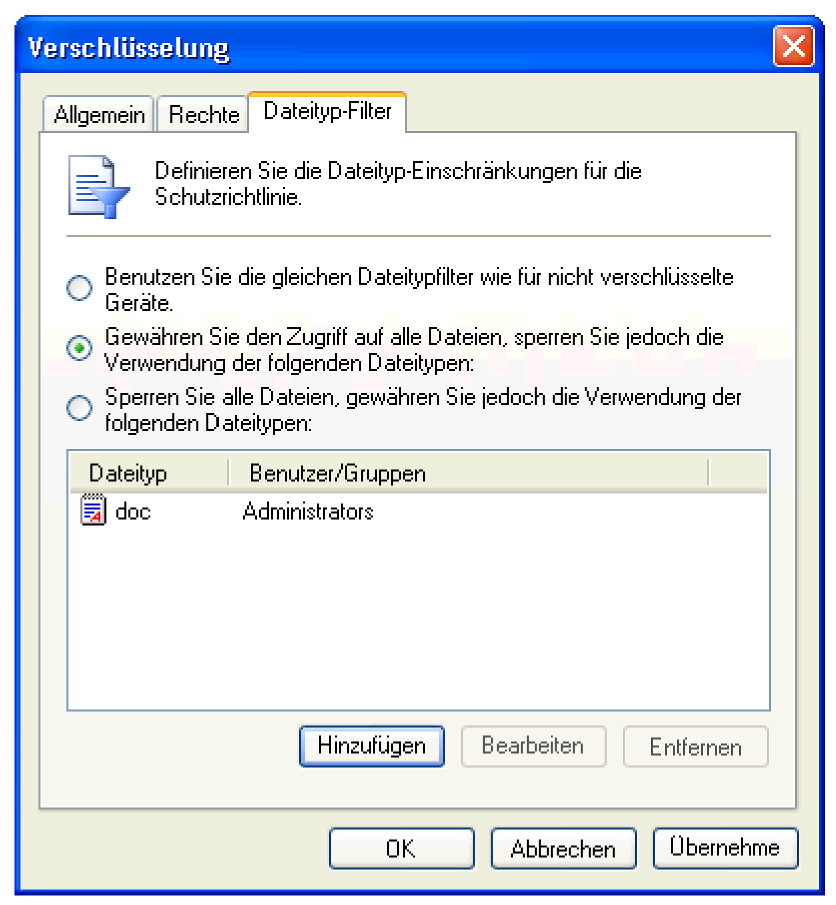
7. Wählen Sie im Dialog **Verschlüsselung** die Registerkarte **Allgemein**. Aktivieren bzw. deaktivieren Sie das Kontrollkästchen **Aktivieren Sie die Erkennung von mit Windows 7 BitLocker To Go verschlüsselten Geräten**, um die Verwendung von Geräten, die mit BitLocker To Go verschlüsselt wurden, zuzulassen oder zu blockieren.




*Screenshot 11 - Verschlüsselungsoptionen - Registerkarte „Berechtigungen"*

8. Falls die BitLocker To Go-Option aktiviert ist, wechseln Sie auf die Registerkarte **Berechtigungen**.

9. Klicken Sie auf **Hinzufügen**, um die Benutzer/Gruppen festzulegen, die auf diese verschlüsselten Geräte, die von dieser Schutzrichtlinie erkannt wurden, Zugriff haben. Klicken Sie anschließend auf **OK**.




*Screenshot 12 - Verschlüsselungsoptionen - Registerkarte „Dateityp-Filter"*

10. Falls die BitLocker To Go-Option aktiviert ist, wählen Sie die Registerkarte **Dateityp-Filter**, um die zugriffsbeschränkten Dateitypen zu konfigurieren.

11. Wählen Sie die auf diese Schutzrichtlinie anzuwendende Einschränkung aus:

» Benutzen Sie die gleichen Dateitypfilter wie für nicht verschlüsselte Geräte

» Gewähren Sie den Zugriff auf alle Dateien, sperren Sie jedoch die Verwendung der folgenden Dateitypen

» Sperren Sie alle Dateien, gewähren Sie jedoch die Verwendung der folgenden Dateitypen

12. Klicken Sie für die letzten beiden Optionen auf **Hinzufügen…**, und wählen Sie den Dateityp aus dem Dropdown-Menü **Dateityp** aus oder geben Sie ihn ein.

13. Klicken Sie auf **Hinzufügen...**, um die Benutzer/Gruppen festzulegen, die auf diesen Dateityp zugreifen können oder dafür gesperrt sind. Klicken Sie anschließend auf **OK**.

Wiederholen Sie die vorherigen 2 Unterschritte für jeden zu beschränkenden Dateityp.

14. Klicken Sie zweimal auf **OK**.

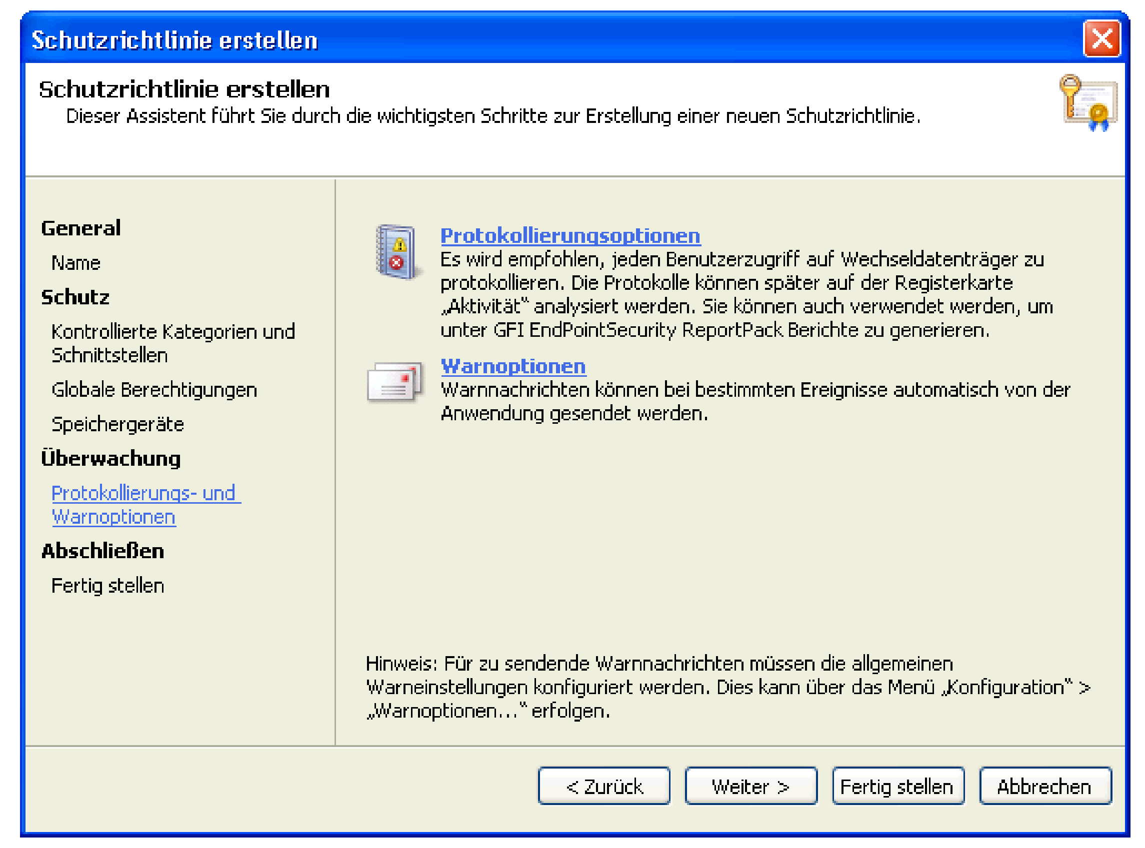
15. Klicken Sie auf **Weiter**.

### *Schritt 6: Konfigurieren der Protokollierungs- und Warnoptionen*

GFI EndPointSecurity bietet Ihnen die Möglichkeit, die Geräte- und Schnittstellennutzung für Analyse- und Berichterstellungszwecke zu protokollieren. Zusätzlich können Sie Alarmtypen konfigurieren, die bei bestimmten Ereignissen an festgelegte Empfänger gesendet werden.



Alarmempfänger sind keine Active Directory (AD)-Benutzer, Benutzergruppen, lokale Benutzer und/oder Benutzerschemen. Es sind von GFI EndPointSecurity erstellte Profilkonten, die Kontaktdetails von Benutzern enthalten, die für Alarme vorgesehen sind. Am besten sollten Alarmempfänger vor der Konfiguration der Alarme erstellt werden. Weitere Informationen zur Erstellung von Benutzern und Gruppen für Benachrichtigungszwecke finden Sie im Kapitel Anpassen von GFI EndPointSecurity unter Konfigurieren der Alarmempfänger.




*Screenshot 13 - Assistent zur Erstellung von Schutzrichtlinien von GFI EndPointSecurity: Protokollierungs- und Warnoptionen*

So konfigurieren Sie Protokollierungs- und Warnoptionen für diese Schutzrichtlinie:

1. Klicken Sie auf den Hyperlink **Protokollierungsoptionen**.




*Screenshot 14 - Protokollierungsoptionen - Registerkarte „Allgemein“*

2. Wählen Sie im Dialog **Protokollierungsoptionen** die Registerkarte **Allgemein**.

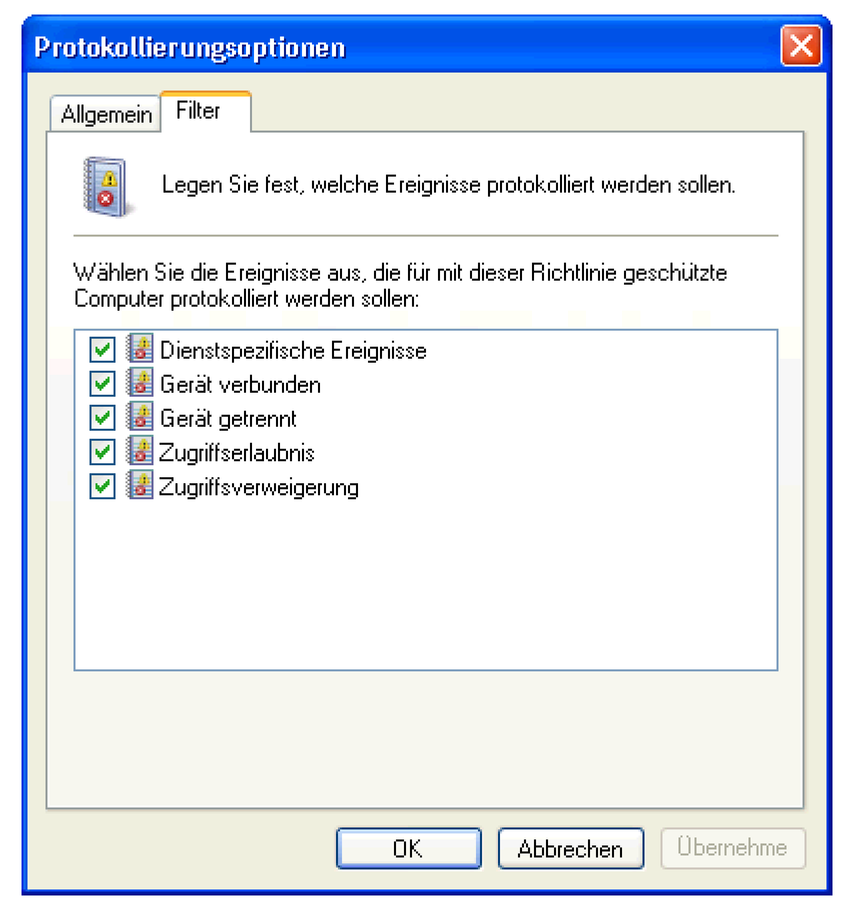
3. Aktivieren bzw. deaktivieren Sie die Speicherorte, an denen von dieser Schutzrichtlinie generierte Ereignisse gespeichert werden sollen:

» **Ereignisse im Windows-Sicherheitsereignisprotokoll protokollieren** – Sie können Ereignisse in der Windows-Ereignisanzeige auf jedem Computer oder über den GFI EventsManager anzeigen, nachdem sie an einer zentralen Stelle gesammelt wurden.

» **Ereignisse in zentraler Datenbank protokollieren** - Sie können Ereignisse auf der untergeordneten Registerkarte „Protokoll-Browser“ in der GFI EndPointSecurity-Verwaltungskonsole anzeigen. Diese Option erfordert die Konfiguration einer zentralen Datenbank. Weitere Informationen zur Konfiguration einer zentralen Datenbank finden Sie im Kapitel **Anpassen von GFI EndPointSecurity** unter **Konfigurieren des Datenbank-Backends**.



Falls beide Optionen aktiviert sind, werden die gleichen Daten an beiden Speicherorten protokolliert.

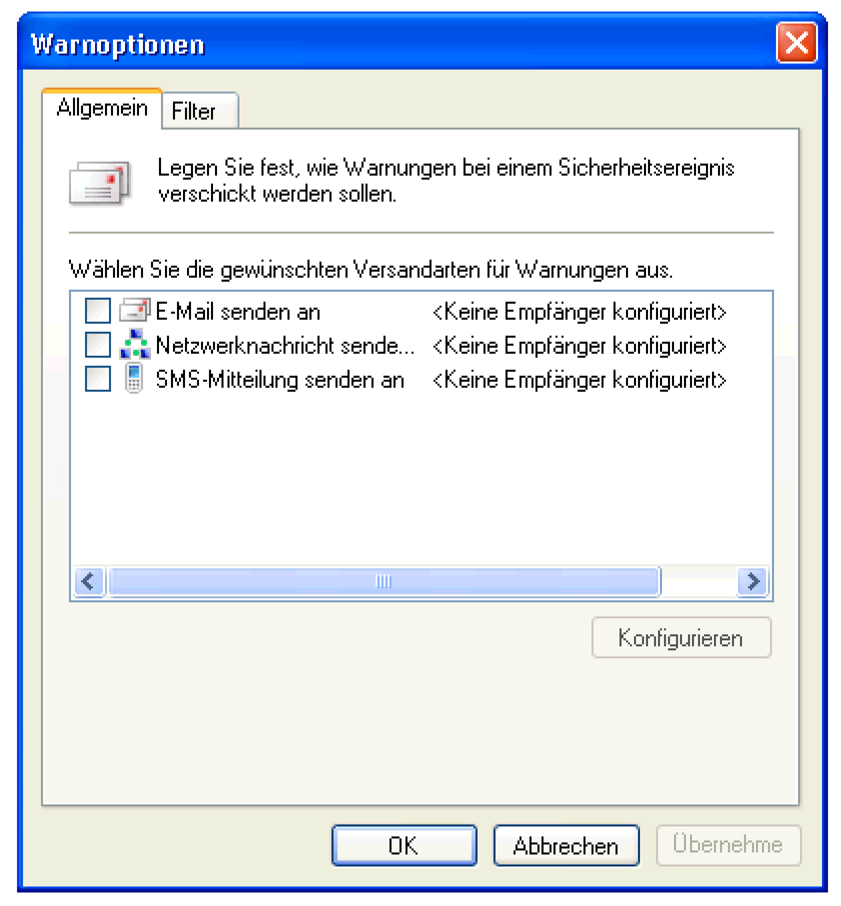



*Screenshot 15 - Protokollierungsoptionen - Registerkarte „Filter"*

4. Wählen Sie auf der Registerkarte **Filter** aus den folgenden Ereignistypen aus, die durch diese Schutzrichtlinie protokolliert werden sollen. Klicken Sie anschließend auf **OK**:

- Dienstereignisse,
- Ereignis – Geräteanschluss,
- Ereignis – Gerätetrennung,
- Ereignis – Zugriffserlaubnis,
- Ereignis – Zugriffsverweigerung.

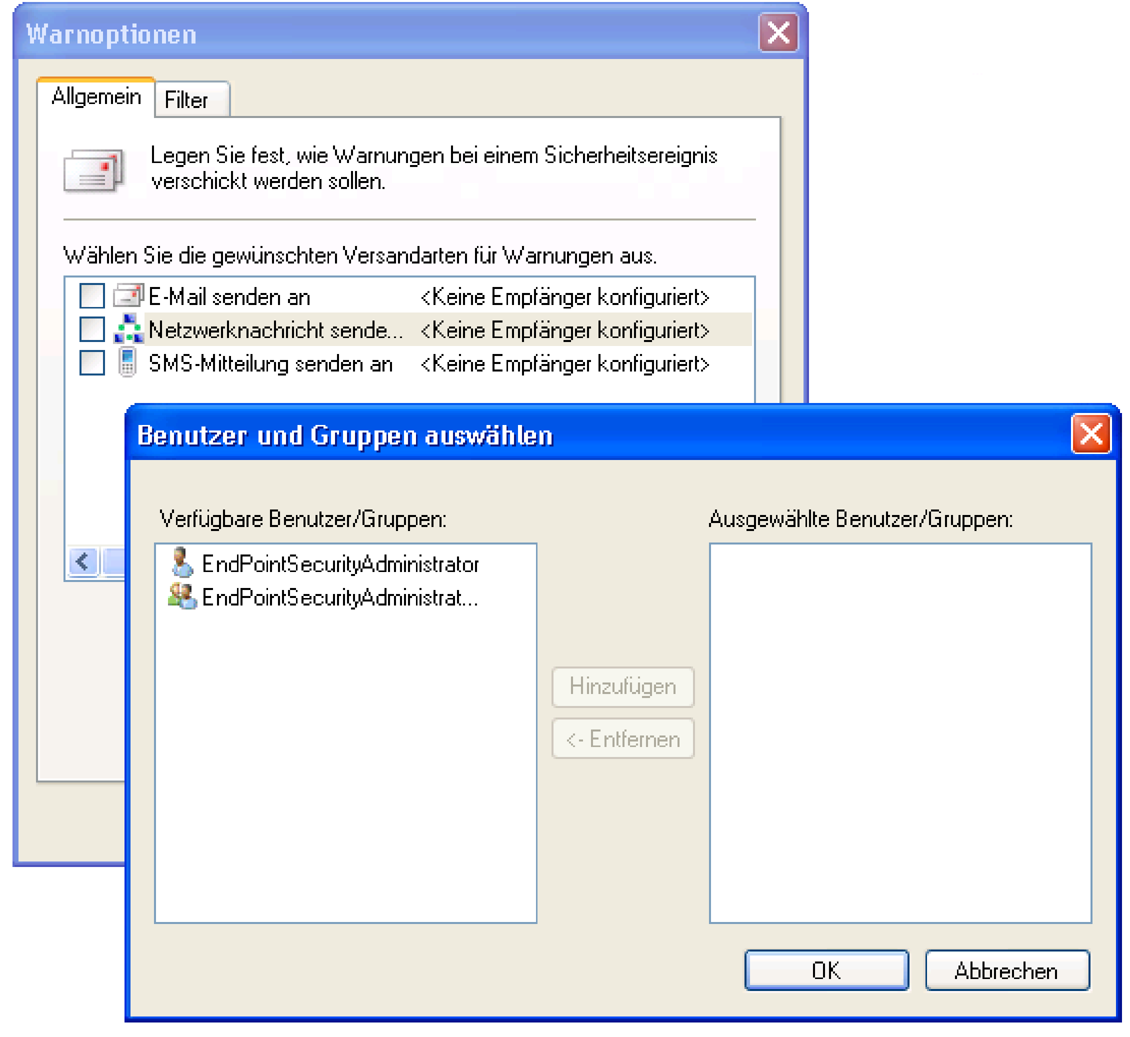
5. Klicken Sie auf den Hyperlink **Warnoptionen**.




*Screenshot 16 - Warnoptionen - Registerkarte „Allgemein"*

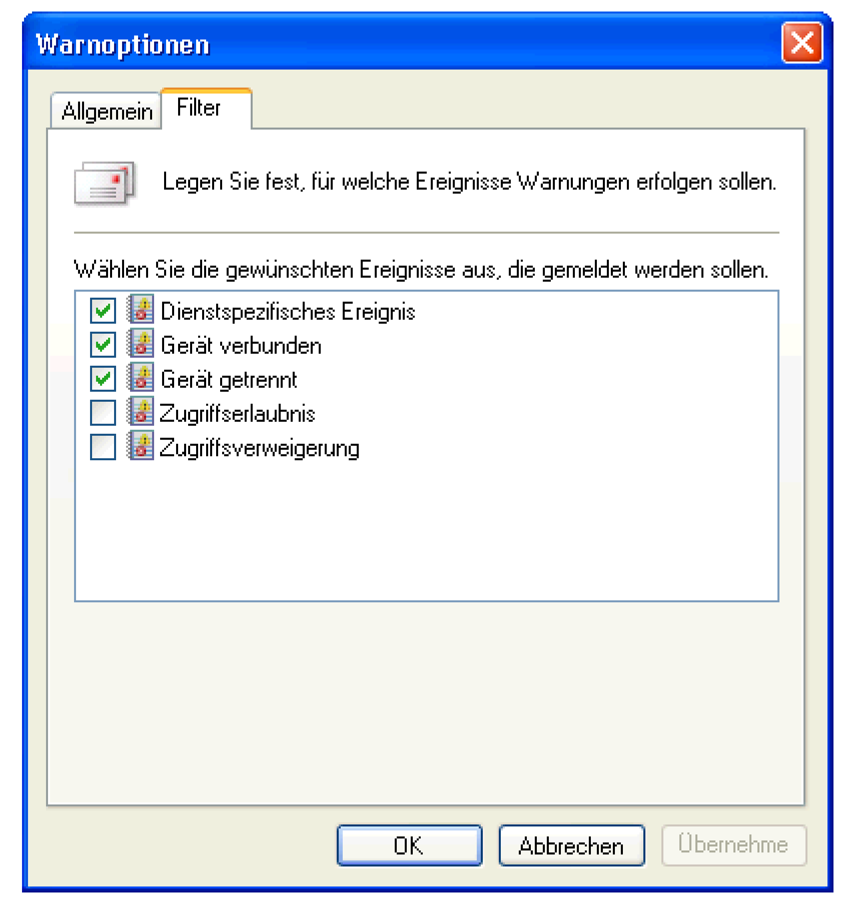
6. Wählen Sie im Dialog **Warnoptionen** die Registerkarte **Allgemein**, und wählen Sie die Alarmtypen, die an Alarmempfänger gesendet werden sollen:

- E-Mail-Warnungen,
- Netzwerknachrichten,
- SMS-Nachrichten.




*Screenshot 17 - Warnoptionen - Konfigurieren von Benutzern und Gruppen*

7. Markieren Sie für jeden aktivierten Alarm den Alarmtyp, und klicken Sie auf **Konfigurieren**, um die Benutzer/Gruppen festzulegen, an die der Alarm gesendet werden sollen. Klicken Sie anschließend auf **OK**.



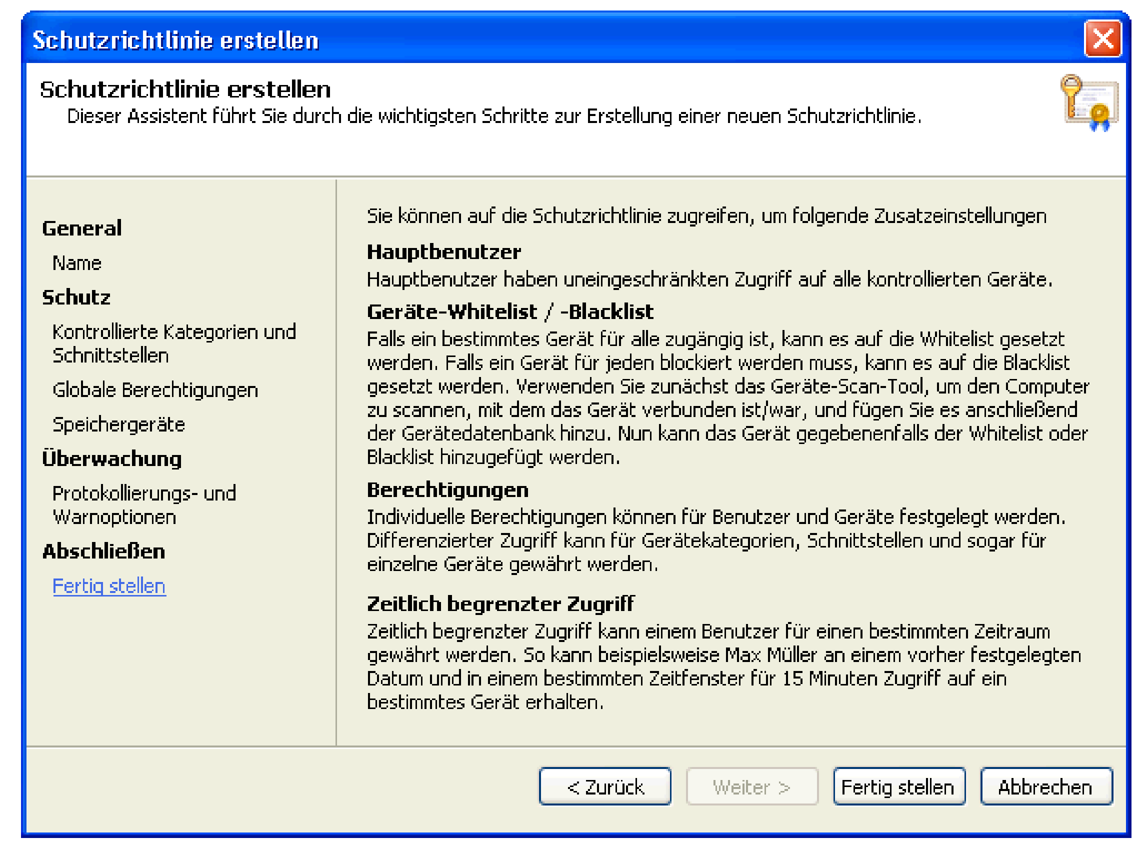

*Screenshot 18 - Warnoptionen - Registerkarte „Filter“*

8. Wählen Sie auf der Registerkarte **Filter** aus den folgenden Ereignistypen aus, für die Alarme durch diese Schutzrichtlinie gesendet werden sollen. Klicken Sie anschließend auf **OK**:

- Dienstereignisse,
- Ereignis – Geräteanschluss,
- Ereignis – Gerätetrennung,
- Ereignis – Zugriffserlaubnis,
- Ereignis – Zugriffsverweigerung.

9. Klicken Sie auf **Weiter**.

### Schritt 7: Fertig stellen des Assistenten




*Screenshot 19 - Assistent zur Erstellung von Schutzrichtlinien von GFI EndPointSecurity: Fertig stellen*

So stellen Sie den Assistenten für diese Schutzrichtlinie fertig:

1. Prüfen Sie die Seite der Richtlinien.
2. Klicken Sie auf **Fertig stellen**, um den Assistenten zu schließen.

# 4 Bereitstellen von Schutzrichtlinien

## 4.1 Einführung

Nach der Erstellung einer neuen Schutzrichtlinie muss diese auf den zu kontrollierenden Computern bereitgestellt werden. In diesem Kapitel werden folgende Aspekte behandelt:

- Einen zu kontrollierenden Computer der Computerliste hinzufügen
- Eine Schutzrichtlinie einem zu kontrollierenden Computer zuweisen
- Eine Schutzrichtlinie auf einem zu kontrollierenden Computer bereitstellen
- Die Bereitstellung einer Schutzrichtlinie auf einem zu kontrollierenden Computer prüfen



Vor der Bereitstellung können Sie die Einstellungen Ihrer Schutzrichtlinie modifizieren. Weitere Informationen zur Konfiguration bestimmter Einstellungen finden Sie im Kapitel **Anpassen von Schutzrichtlinien** in diesem Handbuch.

## 4.2 Hinzufügen eines zu kontrollierenden Computer zur Computerliste

GFI EndPointSecurity bietet Ihnen die Möglichkeit, die Computer festzulegen, auf denen Agenten und Schutzrichtlinien bereitgestellt werden sollen. Sie können Computer der Liste **Computer** folgendermaßen hinzufügen:

- Manuell der Liste hinzufügen,
- Mithilfe der automatischen Suche.

Dieser Abschnitt beschreibt, wie ein zu kontrollierender Computer manuell in die Computerliste aufgenommen werden kann.

Weitere Informationen zur automatischen Suche von zu kontrollierenden Computern und dem Hinzufügen zur Computerliste finden Sie im Kapitel **Anpassen von GFI EndPointSecurity** unter **Konfigurieren der automatischen Suche**.

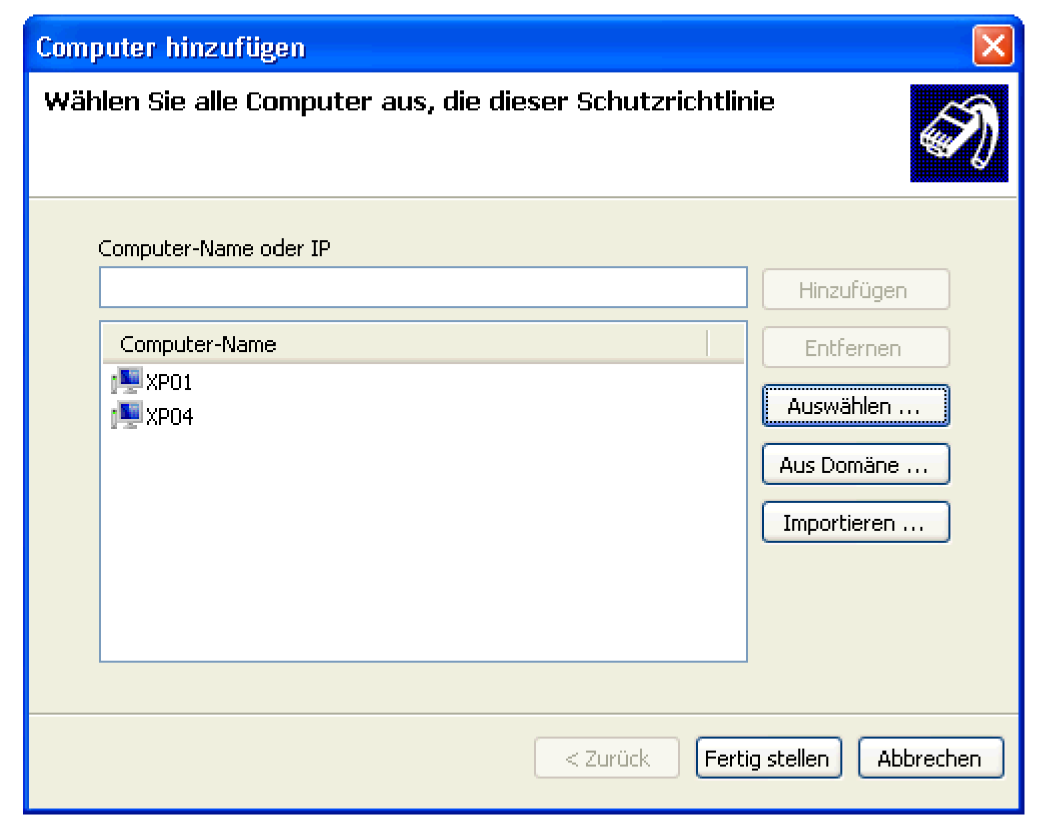
### 4.2.1 Hinzufügen eines zu kontrollierenden Computers

So fügen Sie einen zu kontrollierenden Computer der Computerliste hinzu:

1. Klicken Sie in der GFI EndPointSecurity-Verwaltungskonsole auf die Registerkarte **Konfiguration**.

2. Klicken Sie auf die untergeordnete Registerkarte **Computer**.

3. Klicken Sie im linken Bereich im Abschnitt **Allgemeine Aufgaben** auf den Hyperlink **Computer hinzufügen...**.

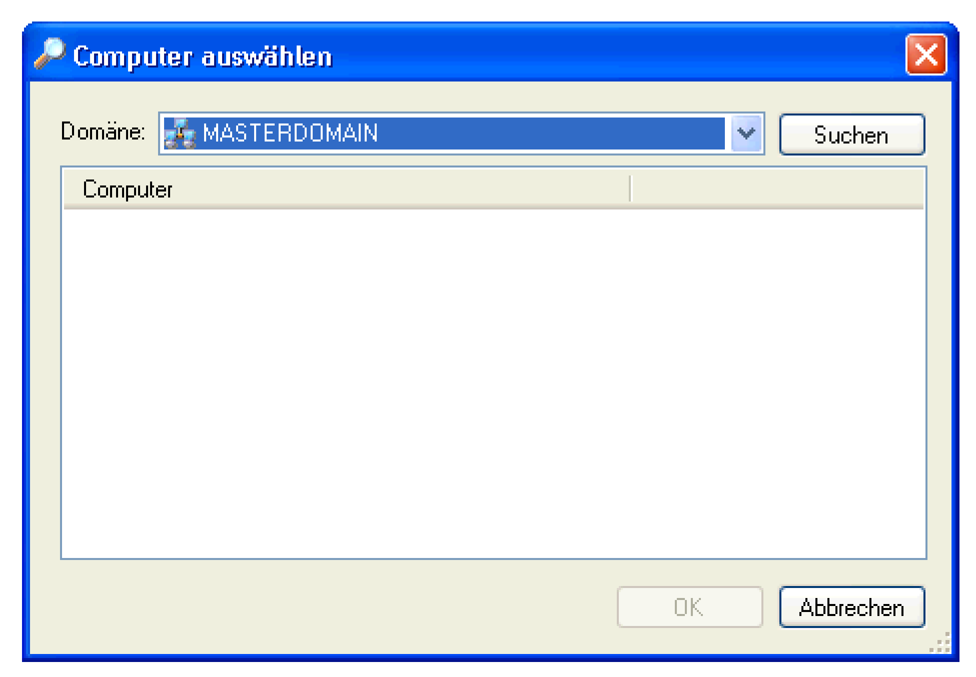



*Screenshot 20 - Optionen zum Hinzufügen von Computern*

4. Im Dialog **Computer hinzufügen**:

» Option 1: Geben Sie den Namen / die IP-Adresse des zu kontrollierenden Computers ein, und klicken Sie auf **Hinzufügen**.

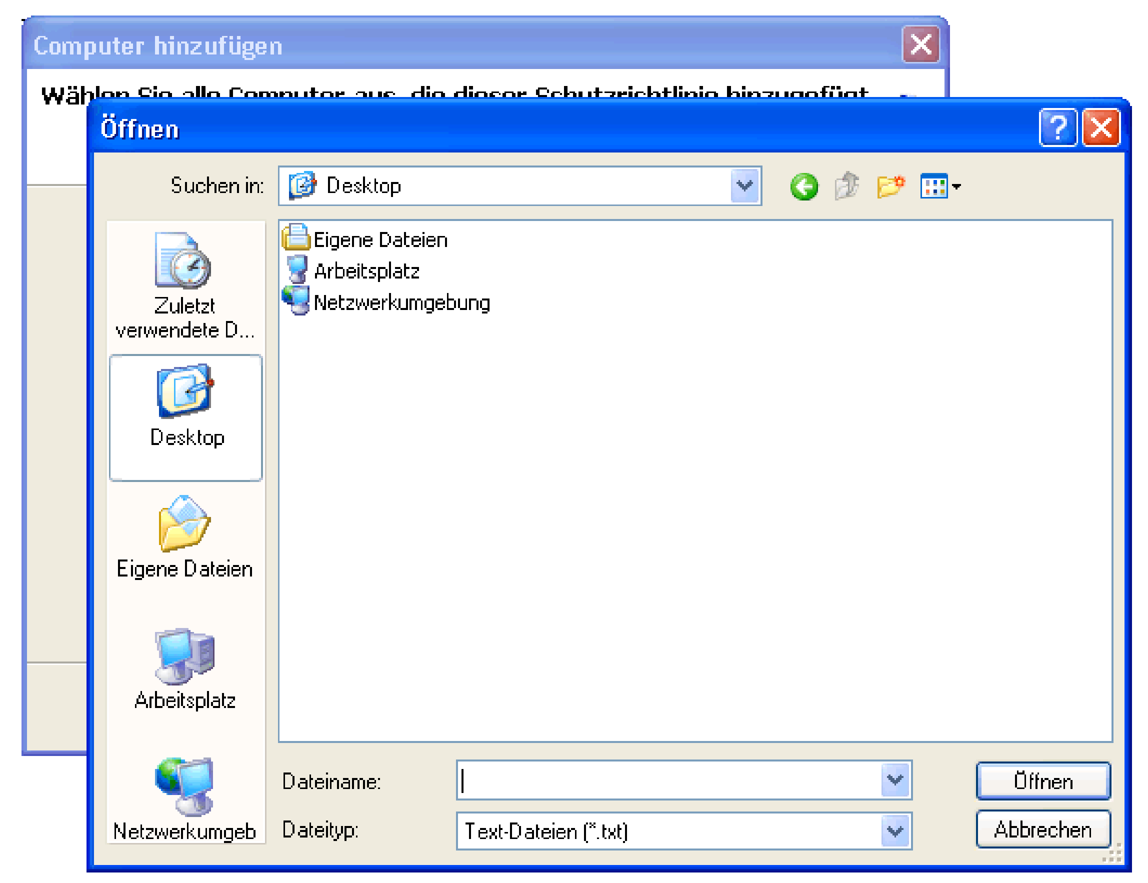
Wiederholen Sie den vorherigen Unterschritt für jeden zu kontrollierenden Computer, der dieser Schutzrichtlinie hinzugefügt werden soll.




*Screenshot 21 - Optionen zur Computerauswahl*

» Option 2: Klicken Sie auf **Auswählen…**. Wählen Sie im Dialog **Computer auswählen** die relevante **Domäne** aus dem Dropdown-Menü aus, und klicken Sie auf **Suche**. Aktivieren Sie die gewünschten Computer, und klicken Sie auf **OK**.

» Option 3: Klicken Sie auf **Von Domäne…**. Geben Sie die gewünschten Computer der Domäne an, wo sich die GFI EndPointSecurity-Verwaltungskonsole befindet.




*Screenshot 22 - Optionen zum Computerimport*

» Option 4: Klicken Sie auf **Importieren…**. Suchen Sie die Textdatei, die eine Liste der zu importierenden Computer enthält.

5. Klicken Sie auf **Fertig stellen**.

### 4.2.2 Konfigurieren der Anmeldeinformationen

GFI EndPointSecurity muss sich an den zu kontrollierenden Computern anmelden, um:

» Agenten und Aktualisierungen für Schutzrichtlinien bereitzustellen,

» den Schutzstatus der zu kontrollierenden Computer zu kontrollieren.

Hierfür ist erforderlich, dass GFI EndPointSecurity unter einem Konto mit administrativen Berechtigungen für die im Netzwerk zu kontrollierenden Computer läuft (z. B. Domänenadministrator-Konto).

So legen Sie die Anmeldeinformationen für einen zu kontrollierenden Computer fest:

1. Klicken Sie in der GFI EndPointSecurity-Verwaltungskonsole auf die Registerkarte **Konfiguration**.

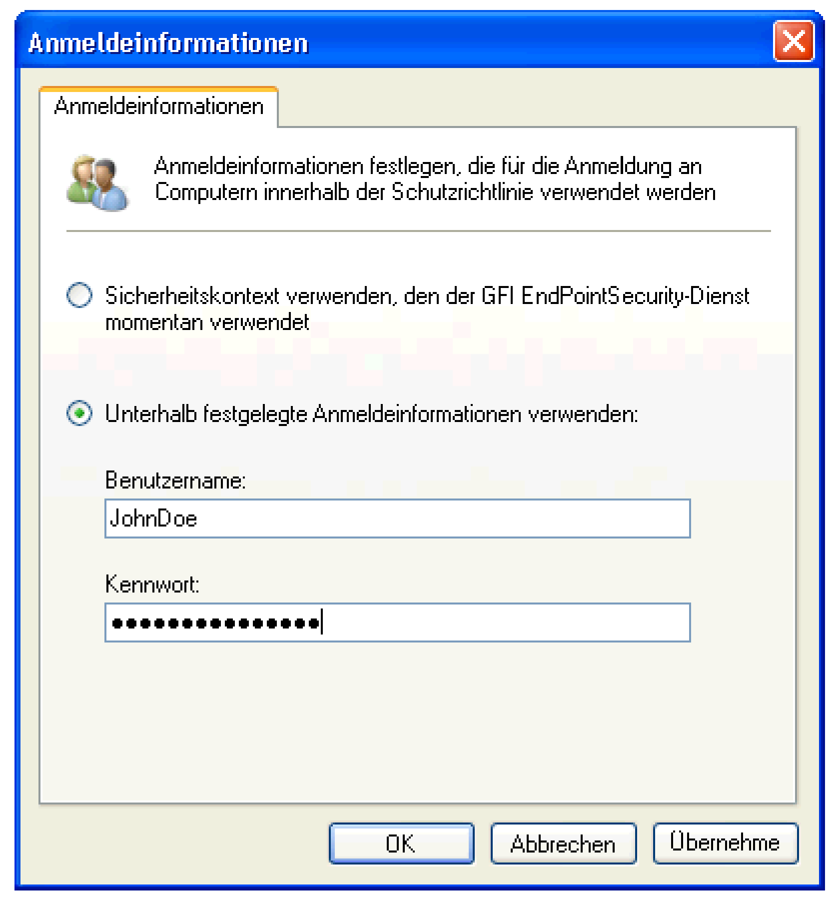
2. Klicken Sie auf die untergeordnete Registerkarte **Computer**.

3. Markieren Sie die gewünschten zu kontrollierenden Computer.



Falls sich GFI EndPointSecurity bei mehr als einem Computer auf die gleiche Weise anmelden kann, können Sie alle gewünschten zu kontrollierenden Computer gleichzeitig markieren und anschließend die Anmeldeinformationen für die ausgewählten Computer festlegen.

4. Klicken Sie im linken Bereich im Abschnitt **Aktionen** auf den Hyperlink **Anmeldeinformationen festlegen....**




*Screenshot 23 - Optionen für Anmeldeinformationen*

5. Wählen Sie im Dialog **Anmeldeinformationen** die Anmeldeinformationen aus, die GFI EndPointSecurity für die physische Anmeldung bei den zu kontrollierenden Computern benötigt. Klicken Sie anschließend auf **OK**.



GFI EndPointSecurity verwendet standardmäßig die Anmeldeinformationen des aktuell angemeldeten Benutzers, unter dem die GFI EndPointSecurity ausgeführt wird.

## 4.3 Zuweisen einer Schutzrichtlinie

Im nächsten Schritt werden die relevanten Berechtigungen für Geräte- und Schnittstellenzugriff mit den jeweiligen Computern verknüpft. Dies erfolgt durch die Zuweisung von Schutzrichtlinien an zu kontrollierende Computer.



Zu kontrollierenden Computer kann nur jeweils eine Schutzrichtlinie zugewiesen werden.

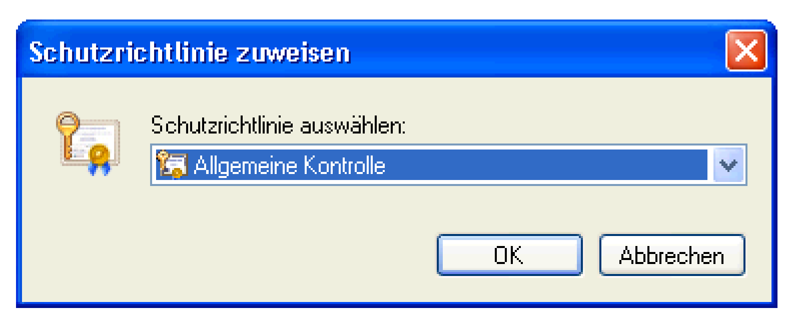
So weisen Sie eine Schutzrichtlinie einem zu kontrollierenden Computer zu:

1. Klicken Sie in der GFI EndPointSecurity-Verwaltungskonsole auf die Registerkarte **Konfiguration**.
2. Klicken Sie auf die untergeordnete Registerkarte **Computer**.
3. Markieren Sie die gewünschten zu kontrollierenden Computer.



Falls die gleiche Schutzrichtlinie mehreren Computer zugewiesen werden soll, können Sie alle gewünschten zu kontrollierenden Computer gleichzeitig markieren und anschließend die Schutzrichtlinie für die ausgewählten Computer festlegen.

4. Klicken Sie im linken Bereich im Abschnitt **Aktionen** auf den Hyperlink **Richtlinie zuweisen...**.




*Screenshot 24 - Optionen zur Zuweisung von Schutzrichtlinien*

5. Wählen Sie im Dialog **Schutzrichtlinie zuweisen** die erforderliche Schutzrichtlinie aus dem Dropdown-Menü aus, und klicken Sie auf **OK**.

## 4.4 Bereitstellen einer Schutzrichtlinie

Im letzten Schritt werden die relevanten Berechtigungen für Geräte- und Schnittstellenzugriff auf den jeweiligen Computern angewendet. Dies erfolgt durch die Bereitstellung von Schutzrichtlinien auf zu kontrollierenden Computern mithilfe einer der folgenden Methoden:

- Sofort bereitstellen,
- Zeitplan für Bereitstellung festlegen,
- Über Active Directory bereitstellen.



Bei der ersten Bereitstellung einer Schutzrichtlinie wird automatisch ein GFI EndPointSecurity-Agent auf dem zu kontrollierenden Computer installiert. Bei weiteren Bereitstellungen der gleichen Schutzrichtlinie wird der Agent aktualisiert, nicht neu installiert.

### 4.4.1 Sofort bereitstellen

So stellen Sie eine Schutzrichtlinie sofort auf einem zu kontrollierenden Computer bereit:

1. Klicken Sie in der GFI EndPointSecurity-Verwaltungskonsole auf die Registerkarte **Konfiguration**.

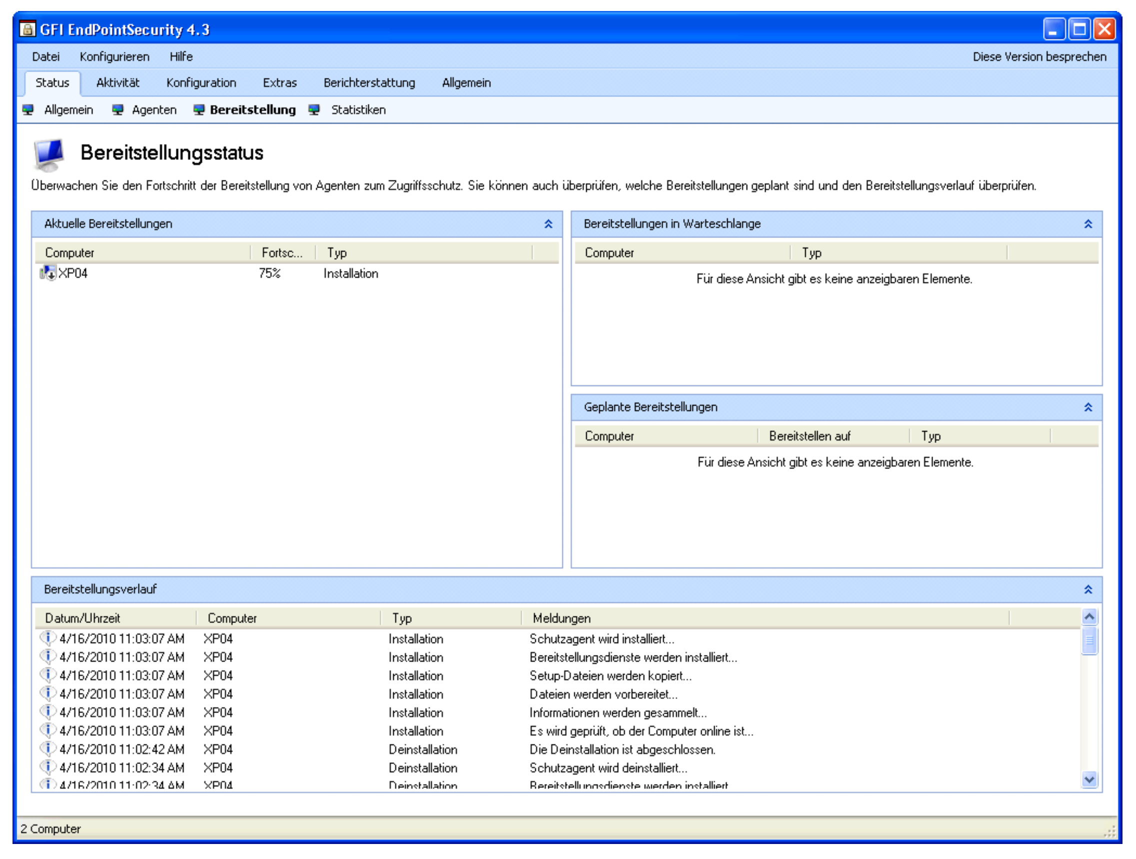
2. Klicken Sie auf die untergeordnete Registerkarte **Computer**.

3. Markieren Sie die gewünschten zu kontrollierenden Computer.



Falls mehr als eine Bereitstellung erforderlich ist, können Sie alle gewünschten zu kontrollierenden Computer gleichzeitig markieren und anschließend die Schutzrichtlinie für den ausgewählten Computer bereitstellen.

4. Klicken Sie im linken Bereich im Abschnitt **Aktionen** auf den Hyperlink **Bereitstellen...**. Die Ansicht sollte automatisch zu **Status** ► **Bereitstellung** wechseln.




*Screenshot 25 - Untergeordnete Registerkarte „Bereitstellung“*

### 4.4.2 Zeitplan für Bereitstellung festlegen

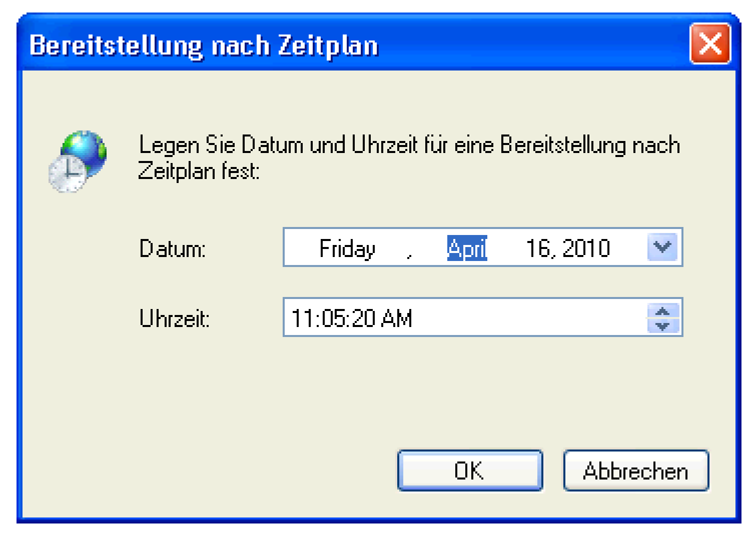
So planen Sie die Bereitstellung einer Schutzrichtlinie auf einem zu kontrollierenden Computer:

1. Klicken Sie in der GFI EndPointSecurity-Verwaltungskonsole auf die Registerkarte **Konfiguration**.
2. Klicken Sie auf die untergeordnete Registerkarte **Computer**.
3. Markieren Sie die gewünschten zu kontrollierenden Computer.



Falls mehr als eine Bereitstellung erforderlich ist, können Sie alle gewünschten zu kontrollierenden Computer gleichzeitig markieren und anschließend die Schutzrichtlinie für den ausgewählten Computer bereitstellen.

4. Klicken Sie im linken Bereich im Abschnitt **Aktionen** auf den Hyperlink **Zeitplan für Bereitstellung festlegen...**.




*Screenshot 26 - Optionen für die Planung einer Bereitstellung*

5. Wählen Sie im Dialog **Zeitplan für Bereitstellung festlegen** das Datum und die Uhrzeit für die Bereitstellung aus. Klicken Sie anschließend auf **OK**.



Falls der zu kontrollierende Computer offline ist, erfolgt eine Stunde später automatisch ein erneuter Versuch. GFI EndPointSecurity versucht die Richtlinie so lange jede Stunde bereitzustellen, bis der zu kontrollierende Computer wieder online ist.

### 4.4.3 Über Active Directory bereitstellen

Standardmäßige Schutzrichtlinien können auch über ein Windows Installer-Paket (MSI-Installationsdatei) mit Hilfe von Active Directory-Gruppenrichtlinien auf zu kontrollierenden Computern in Ihrer Domäne bereitgestellt werden.

So erstellen Sie ein Windows Installer-Paket:

1. Klicken Sie in der GFI EndPointSecurity-Verwaltungskonsole auf die Registerkarte **Konfiguration**.

2. Klicken Sie auf die untergeordnete Registerkarte **Schutzrichtlinien**.

3. Wählen Sie im linken Bereich die Schutzrichtlinie aus, für die ein Windows Installer-Paket erstellt werden soll.

4. Klicken Sie im rechten Bereich im Abschnitt **Bereitstellung** auf den Hyperlink **Über Active Directory bereitstellen**.

5. Geben Sie den **Dateinamen** der .msi-Datei ein, und suchen Sie den Zielpfad. Klicken Sie anschließend auf **Speichern**.

Weitere Informationen zur Bereitstellung von Software mithilfe von Active Directory-Gruppenrichtlinien unter Microsoft Windows Server 2003 und Microsoft Windows Server 2008 finden Sie unter http://support.microsoft.com/kb/816102.

## 4.5 Überprüfen der Bereitstellung einer Schutzrichtlinie

Nach der Bereitstellung einer Schutzrichtlinie wird empfohlen, diese zu überprüfen, und die Zuweisung der richtigen Schutzrichtlinie auf dem richtigen Computer zu bestätigen.

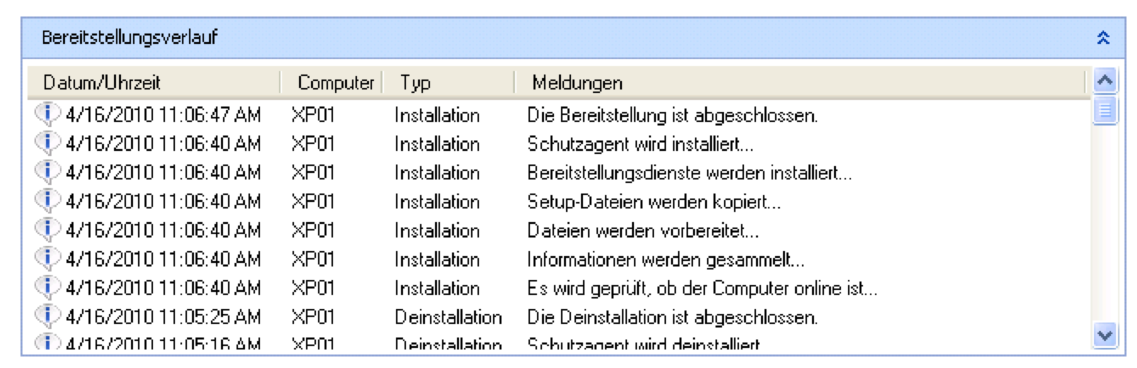
### 4.5.1 Bereitstellungsverlauf

Verwenden Sie die Informationen aus dem Bereich **Bereitstellungsverlauf**, um zu bestimmen, ob die Bereitstellung für jeden zu kontrollierenden Computer erfolgreich war oder ob Fehler vorliegen.

So zeigen Sie den Bereitstellungsverlauf an:

1. Klicken Sie in der GFI EndPointSecurity-Verwaltungskonsole auf die Registerkarte **Status**.

2. Klicken Sie auf die untergeordnete Registerkarte **Bereitstellung**.



Bereitstellungsverlauf

| Datum/Uhrzeit | Computer | Typ | Meldungen |
|---|---|---|---|
| 4/16/2010 11:06:47 AM | XP01 | Installation | Die Bereitstellung ist abgeschlossen. |
| 4/16/2010 11:06:40 AM | XP01 | Installation | Schutzagent wird installiert... |
| 4/16/2010 11:06:40 AM | XP01 | Installation | Bereitstellungsdienste werden installiert... |
| 4/16/2010 11:06:40 AM | XP01 | Installation | Setup-Dateien werden kopiert... |
| 4/16/2010 11:06:40 AM | XP01 | Installation | Dateien werden vorbereitet... |
| 4/16/2010 11:06:40 AM | XP01 | Installation | Informationen werden gesammelt... |
| 4/16/2010 11:06:40 AM | XP01 | Installation | Es wird geprüft, ob der Computer online ist... |
| 4/16/2010 11:05:25 AM | XP01 | Deinstallation | Die Deinstallation ist abgeschlossen. |
| 4/16/2010 11:05:16 AM | XP01 | Deinstallation | Schutzagent wird deinstalliert |

*Screenshot 27 - Bereich „Bereitstellungsverlauf"*

3. Überprüfen Sie im Bereich **Bereitstellungsverlauf** den erfolgreichen Abschluss der Aktualisierung auf dem lokalen Computer.

Weitere Informationen zum Bereich „Bereitstellungsverlauf" finden Sie im Kapitel **Statusüberwachung** unter **Bereitstellungsverlauf**.

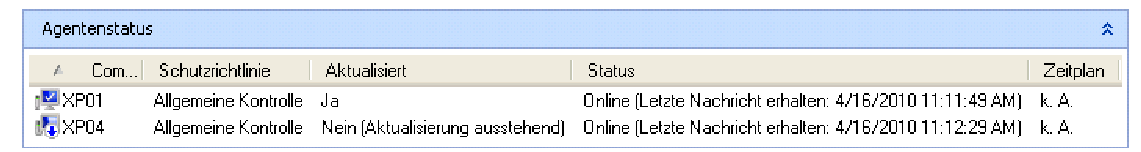
## 4.5.2 Agentenstatus

Verwenden Sie die Informationen aus dem Bereich **Agentenstatus**, um den Status alle Bereitstellungsvorgänge auf den kontrollierten Computern zu bestimmen.

So zeigen Sie den Agentenstatus an:

1. Klicken Sie in der GFI EndPointSecurity-Verwaltungskonsole auf die Registerkarte **Status**.

2. Klicken Sie auf die untergeordnete Registerkarte **Agenten**.



Agentenstatus

| Com... | Schutzrichtlinie | Aktualisiert | Status | Zeitplan |
|---|---|---|---|---|
| XP01 | Allgemeine Kontrolle | Ja | Online (Letzte Nachricht erhalten: 4/16/2010 11:11:49 AM) | k. A. |
| XP04 | Allgemeine Kontrolle | Nein (Aktualisierung ausstehend) | Online (Letzte Nachricht erhalten: 4/16/2010 11:12:29 AM) | k. A. |

*Screenshot 28 - Bereich „Agentenstatus"*

3. Bestätigen Sie im Bereich **Agentenstatus** die erfolgreiche Zuweisung der richtigen Schutzrichtlinie auf den zu kontrollierenden Computern und dass die Agentenbereitstellung auf dem neuesten Stand ist.



Jeder Agent sendet regelmäßig seinen Onlinestatus an die Hauptinstallation von GFI EndPointSecurity. Falls diese Daten nicht von der Hauptinstallation empfangen werden, wird der Agent als offline angesehen.



Falls ein zu kontrollierender Computer offline ist, erfolgt eine Stunde später automatisch ein erneuter Versuch. GFI EndPointSecurity versucht die Richtlinie so lange jede Stunde bereitzustellen, bis der zu kontrollierende Computer wieder online ist.

Weitere Informationen zum Bereich „Agentenstatus" finden Sie im Kapitel **Statusüberwachung** unter **Untergeordnete Registerkarte „Agenten"**.

# 5 Überwachen der Geräteaktivität

## 5.1 Einführung

GFI EndPointSecurity ermöglicht die Nachverfolgung aller Ereignisse, die durch GFI EndPointSecurity-Agenten auf kontrollierten Computern verursacht werden. Dies kann über folgende Elemente erfolgen:

- Untergeordnete Registerkarte „Statistik“
- Registerkarte „Aktivität“



Falls kein Datenbank-Backend konfiguriert ist, wird auf diesen untergeordneten Registerkarten nichts angezeigt. Weitere Informationen zur Konfiguration einer zentralen Datenbank finden Sie im Kapitel **Anpassen von GFI EndPointSecurity** unter **Konfigurieren des Datenbank-Backends**.



Zum Führen eines Audit-Trails muss die Protokollierung aktiviert sein. Weitere Informationen zur Aktivierung der Protokollierung finden Sie im Kapitel **Anpassen von Schutzrichtlinien** unter **Konfigurieren der Ereignisprotokollierung**.

## 5.2 Statistik

Über die untergeordnete Registerkarte **Statistik** können Sie Trends in der täglichen Geräteaktivität feststellen und eine Statistik zu einzelnen oder allen kontrollierten Computern Ihres Netzwerks abrufen.

GFI EndPointSecurity 4.3

Datei Konfigurieren Hilfe — Diese Version besprechen

Status | Aktivität | Konfiguration | Extras | Berichterstattung | Allgemein

Allgemein | Agenten | Bereitstellung | **Statistiken**

**Statistik**

Kontrollieren Sie die Geräteverwendung für alle Computer, oder wählen Sie einzelne Computer aus der folgenden Liste aus.

Wählen Sie einen Computer aus, um dessen Statistik zur Geräteverwendung anzuzeigen:

Alle Computer

Schutzstatus

12 10 8 6 4 2 0

12:00 AM 4:00 AM 8:00 AM 12:00 PM 4:00 PM 8:00 PM 12:00 AM

Erlaubt
Gesperrt

Verwendung nach Gerätekategorie

| Typ | Erlaubt | Gesperrt | Gesamt |
|---|---|---|---|
| Disketten | 2 | 88 | 90 |
| CD/DVD | 2,305 | 405 | 2,710 |
| Speichergeräte | 1,939 | 5,353 | 7,292 |
| Drucker | 11 | 5 | 16 |
| PDAs | 10 | 7 | 17 |
| Netzwerk-Adapter | 16 | 13 | 29 |
| Modems | 6 | 5 | 11 |
| Bildverarbeitungsgeräte | 5 | 7 | 12 |
| Eingabegeräte (HID) | 4 | 4 | 8 |
| Weitere Geräte | 200 | 23 | 223 |

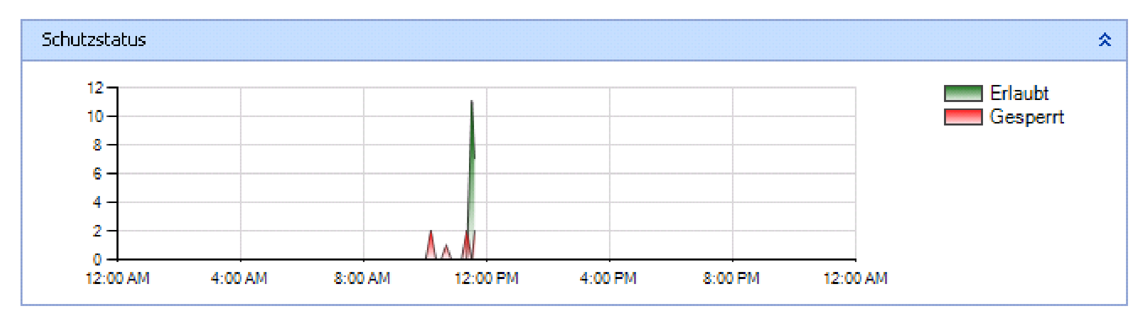
Verwendung nach Schnittstelle

| Typ | Erlaubt | Gesperrt | Gesamt |
|---|---|---|---|
| USB | 1,339 | 1,197 | 2,536 |
| FireWire | 0 | 0 | 0 |
| PCMCIA | 6 | 3 | 9 |
| Bluetooth | 1 | 1 | 2 |
| Seriell und parallel | 0 | 0 | 0 |
| Infrarot | 0 | 0 | 0 |
| Secure Digital (SD) | 1,143 | 4,347 | 5,490 |
| Intern | 2,009 | 362 | 2,371 |

*Screenshot 29 - Untergeordnete Registerkarte „Statistik“*

Klicken Sie für den Zugriff auf die untergeordnete Registerkarte **Statistik** in der GFI EndPointSecurity-Verwaltungskonsole auf die Registerkarte **Status** ► **Statistik**.

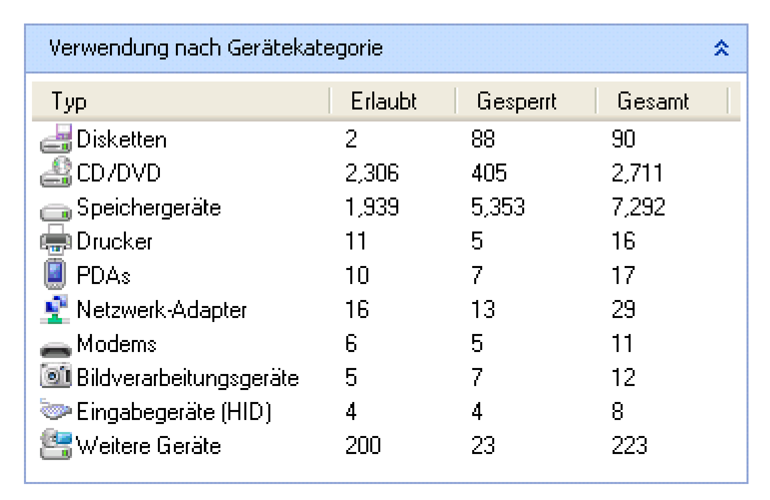
## 5.2.1 Schutzstatus




*Screenshot 30 - Bereich „Schutzstatus“*

In diesem Bereich wird die Geräteaktivität auf Computern im Tagesverlauf anhand eines Diagramms angezeigt. Zugelassene und gesperrte Geräte werden farblich unterschieden. Die bereitgestellten Informationen können für einen einzelnen oder für alle Netzwerkcomputer angezeigt werden.

### 5.2.2 Geräteverwendung durch Gerätetyp

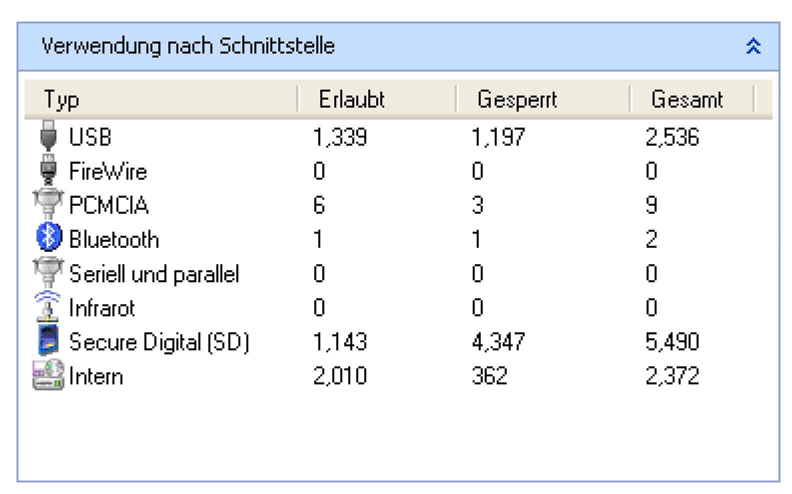

Verwendung nach Gerätekategorie

| Typ | Erlaubt | Gesperrt | Gesamt |
|---|---|---|---|
| Disketten | 2 | 88 | 90 |
| CD/DVD | 2,306 | 405 | 2,711 |
| Speichergeräte | 1,939 | 5,353 | 7,292 |
| Drucker | 11 | 5 | 16 |
| PDAs | 10 | 7 | 17 |
| Netzwerk-Adapter | 16 | 13 | 29 |
| Modems | 6 | 5 | 11 |
| Bildverarbeitungsgeräte | 5 | 7 | 12 |
| Eingabegeräte (HID) | 4 | 4 | 8 |
| Weitere Geräte | 200 | 23 | 223 |

*Screenshot 31 - Bereich „Geräteverwendung durch Gerätetyp“*

Dieser Bereich informiert Sie über zugelassene oder blockierte Verbindungsversuche einzelner Gerätekategorien. Die bereitgestellten Informationen können für einen einzelnen oder für alle Netzwerkcomputer angezeigt werden.

### 5.2.3 Geräteverwendung nach Schnittstelle


Verwendung nach Schnittstelle

| Typ | Erlaubt | Gesperrt | Gesamt |
|---|---|---|---|
| USB | 1,339 | 1,197 | 2,536 |
| FireWire | 0 | 0 | 0 |
| PCMCIA | 6 | 3 | 9 |
| Bluetooth | 1 | 1 | 2 |
| Seriell und parallel | 0 | 0 | 0 |
| Infrarot | 0 | 0 | 0 |
| Secure Digital (SD) | 1,143 | 4,347 | 5,490 |
| Intern | 2,010 | 362 | 2,372 |

*Screenshot 32 - Bereich „Geräteverwendung nach Schnittstelle“*

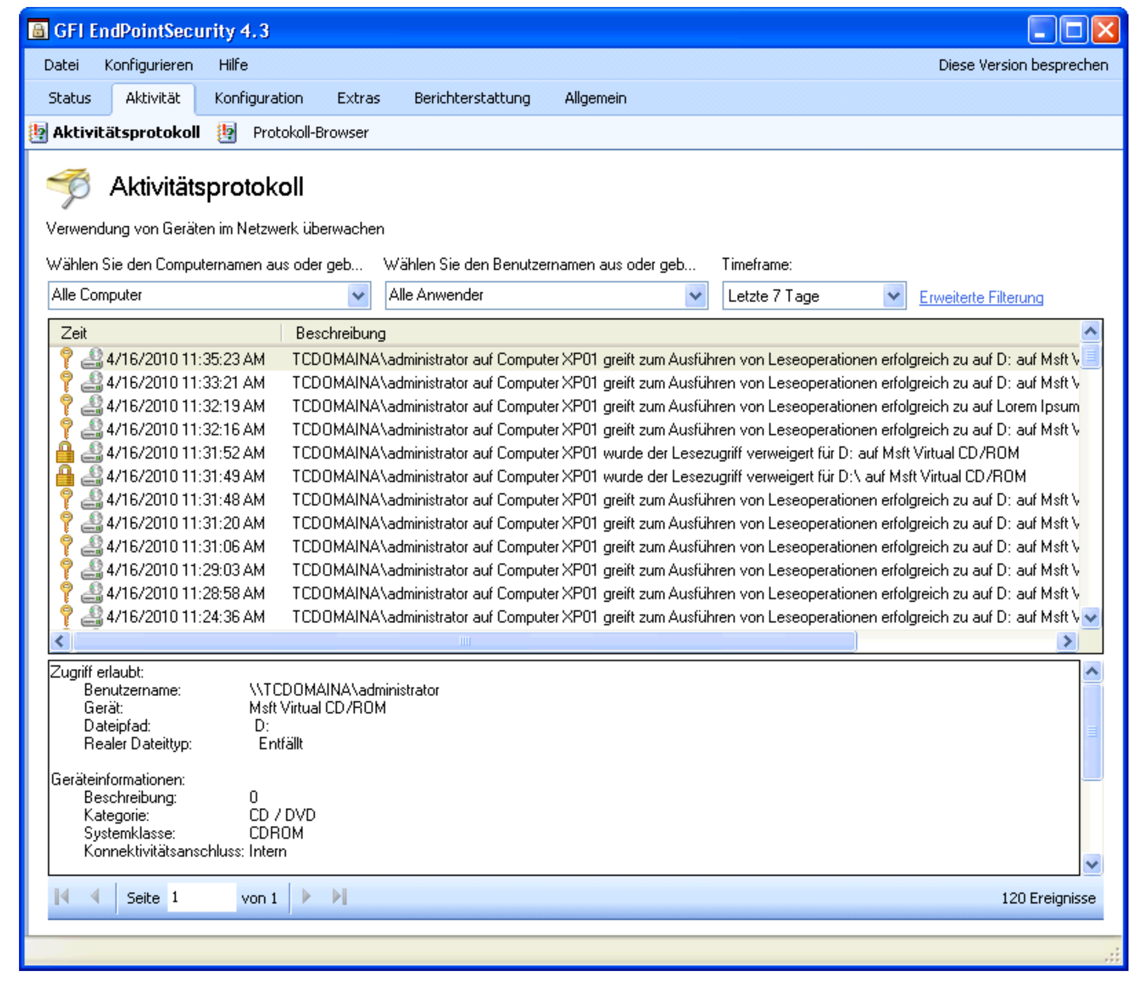
Dieser Bereich informiert Sie über zugelassene oder blockierte Verbindungsversuche über einzelne Schnittstellen. Die bereitgestellten Informationen können für einen einzelnen oder für alle Netzwerkcomputer angezeigt werden.

## 5.3 Aktivität

Verwenden Sie die Registerkarte **Aktivität**, um die Geräteverwendung im Netzwerk und protokollierte Ereignisse für einen bestimmten Computer oder für alle Computer im Netzwerk zu überwachen.

### 5.3.1 Aktivitätsprotokoll

Mit dieser untergeordneten Registerkarte überwachen Sie die Geräte, die im Netzwerk verwendet werden. Wählen Sie den Computer und/oder den Benutzer aus den Dropdown-Menü aus, um das Aktivitätsprotokoll nach Computer und/oder Benutzer zu filtern. Zusätzlich ermöglicht diese Registerkarte, die Liste nach bereitgestellten Zeitfiltern weiter zu filtern.




*Screenshot 33 - Untergeordnete Registerkarte „Aktivitätsprotokoll“*

Klicken Sie für den Zugriff auf die untergeordnete Registerkarte **Aktivitätsprotokoll** in der GFI EndPointSecurity-Verwaltungskonsole auf die Registerkarte **Aktivität** ► **Aktivitätsprotokoll**.

Klicken Sie für weitere Details zu einem Ereignis auf das jeweilige Ereignis. Zusätzliche Informationen werden im Bereich zur Ereignisbeschreibung im unteren Bereich der untergeordneten Registerkarte angezeigt.

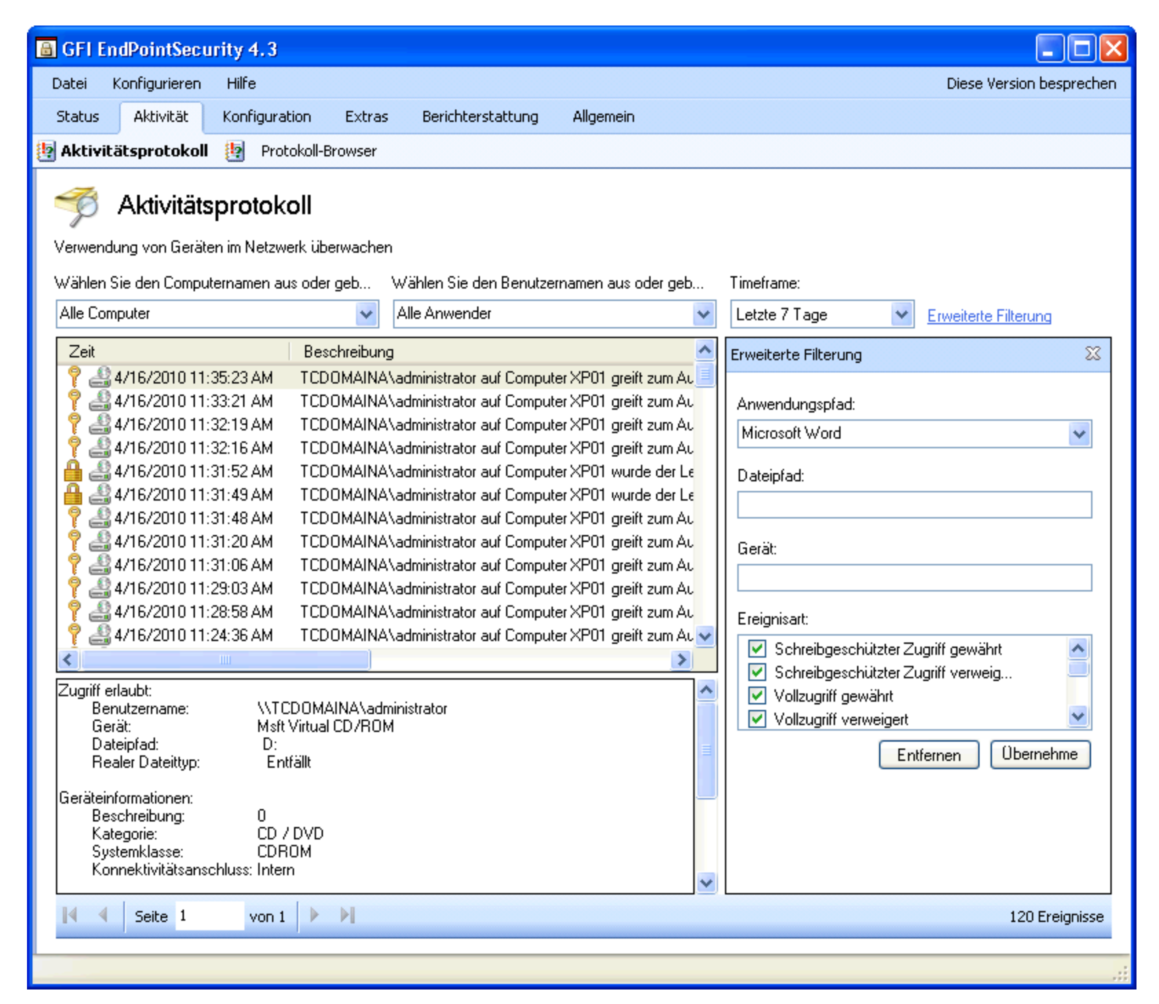
Um die Registerkarte **Aktivitätsprotokoll** den Anforderungen Ihres Unternehmens anzupassen, klicken Sie mit der rechten Maustaste auf die Kopfzeile, und wählen Sie die Spalten, die der Ansicht hinzugefügt oder daraus entfernt werden sollen.

Ziehen Sie zur Änderung der Spaltenreihenfolge eine Spalte am Spaltenkopf an die gewünschten Stelle.

### *Erweiterte Filterung*

Diese Funktion ermöglicht die weitere Filterung der Protokolle zum Geräteverwendungsverlauf mithilfe der folgenden Kriterien:

- Anwendungspfad
- Dateipfad
- Gerät
- Ereignisart



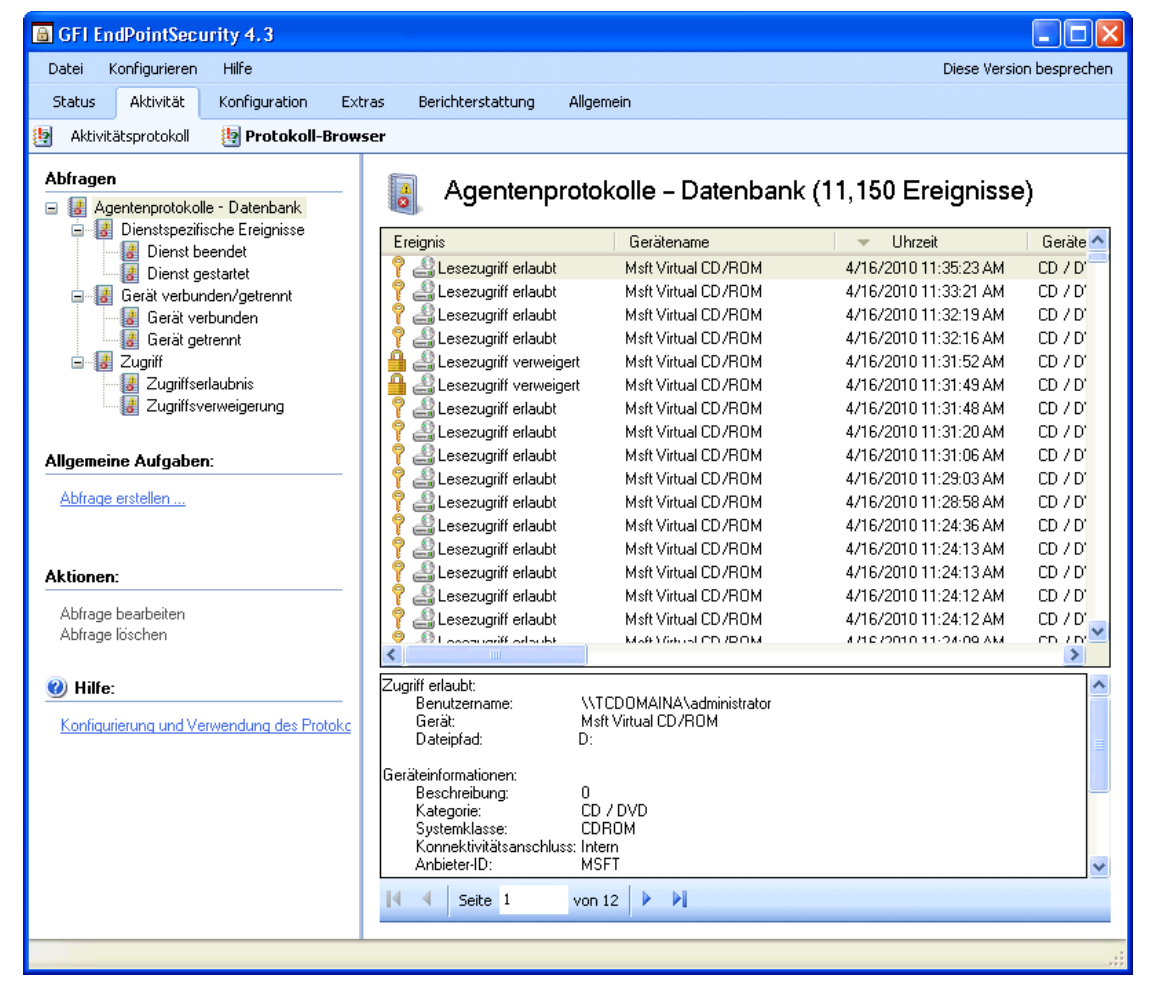

*Screenshot 34 - Untergeordnete Registerkarte „Aktivitätsprotokoll“ - Erweiterte Filterung*

Um auf die erweiterte Filterung des Aktivitätsprotokoll zuzugreifen, klicken Sie auf der untergeordneten Registerkarte **Aktivitätsprotokoll** auf den Hyperlink „Erweiterte Filterung“.

## 5.3.2 Protokoll-Browser

Über diese Registerkarte können Sie im Datenbank-Backend gespeicherte Ereignisse anzeigen und durchsuchen.

Mithilfe des integrierten Abfragegenerators lässt sich die Suche nach bestimmten Ereignissen vereinfachen. Er unterstützt Sie bei der Erstellung eigener Filter zur Filterung von Ereignisdaten und zur Darstellung von Informationen, die für die Suche notwendig sind, ohne dass diese aus dem Datenbank-Backend gelöscht werden.



*Screenshot 35 - Untergeordnete Registerkarte „Protokoll-Browser“*

Klicken Sie für den Zugriff auf die untergeordnete Registerkarte **Protokoll-Browser** in der GFI EndPointSecurity-Verwaltungskonsole auf die Registerkarte **Aktivität** ► **Protokoll-Browser**.

Klicken Sie für weitere Details zu einem Ereignis auf das jeweilige Ereignis. Zusätzliche Informationen werden im Bereich zur Ereignisbeschreibung im unteren Bereich der untergeordneten Registerkarte angezeigt.

## *Erstellen von Ereignisabfragen*

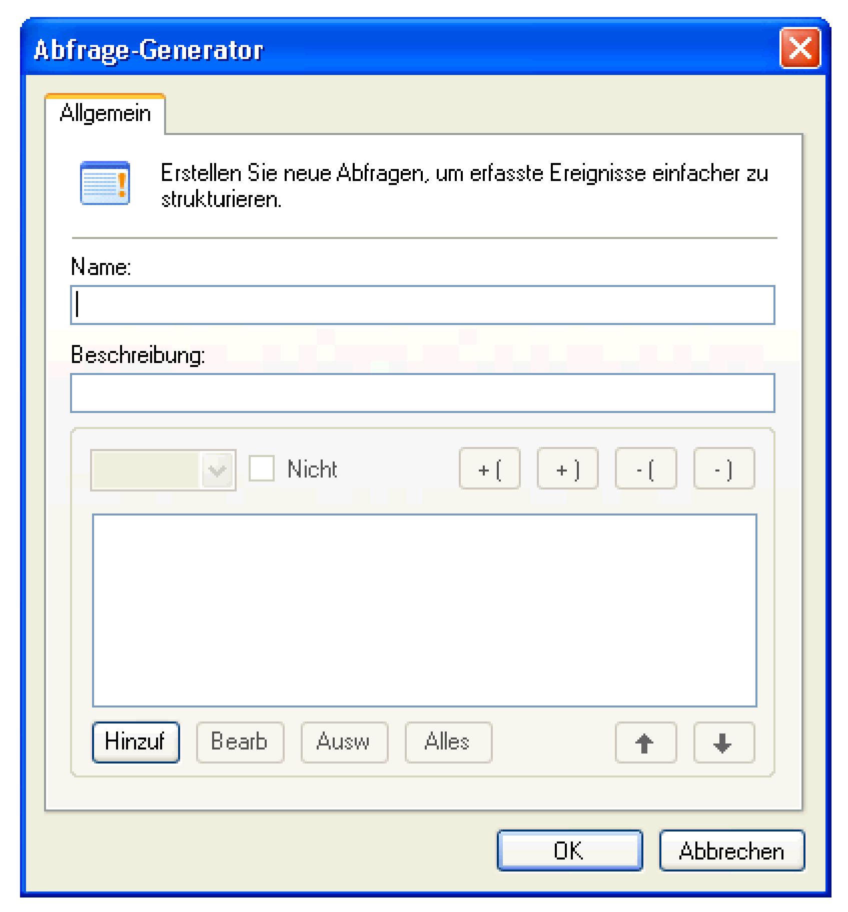
So erstellen Sie eine eigene Ereignisabfrage:

1. Klicken Sie in der GFI EndPointSecurity-Verwaltungskonsole auf die Registerkarte **Aktivität**.

2. Klicken Sie auf die untergeordnete Registerkarte **Protokoll-Browser**.

3. Gehen Sie im linken Bereich auf den Knoten **Agentenprotokolle - Datenbank**.

4. Klicken Sie mit der rechten Maustaste darauf, und wählen Sie **Abfrage erstellen...**.




*Screenshot 36 - Optionen des Abfragegenerators*

5. Geben Sie im Dialog **Abfragegenerators** einen Namen und eine Beschreibung für die neue Abfrage ein.

6. Klicken Sie auf **Hinzufügen...**, konfigurieren Sie die erforderlichen Abfragebedingungen, und klicken Sie auf **OK**. Wiederholen Sie dies, bis alle erforderlichen Abfragebedingungen festgelegt wurden.

7. Klicken Sie auf **OK**, um die Einstellungen fertig zu stellen. Ihre Abfrage wird als Unterknoten des Knotens **Agentenprotokolle - Datenbank** aufgeführt.



Sie können auch die Ergebnisse vorhandener Ereignisabfragen durch Erstellen weiterer spezifischer Unterabfragen filtern. Klicken Sie dazu mit der rechten Maustaste auf die jeweilige Abfrage und wählen Sie **Abfrage erstellen....**

# 6 Statusüberwachung

## 6.1 Einführung

Der Status-Monitor informiert Sie über den aktuellen Status von GFI EndPointSecurity und den Status von Agenten auf kontrollierten Computern. Er liefert dabei Diagramme und statistische Informationen zur Verwendung mobiler Geräte. Der Status-Monitor besteht aus vier untergeordnete Registerkarten:

» Allgemeiner Status

» Agentenstatus

» Bereitstellungsstatus

» Statistik.

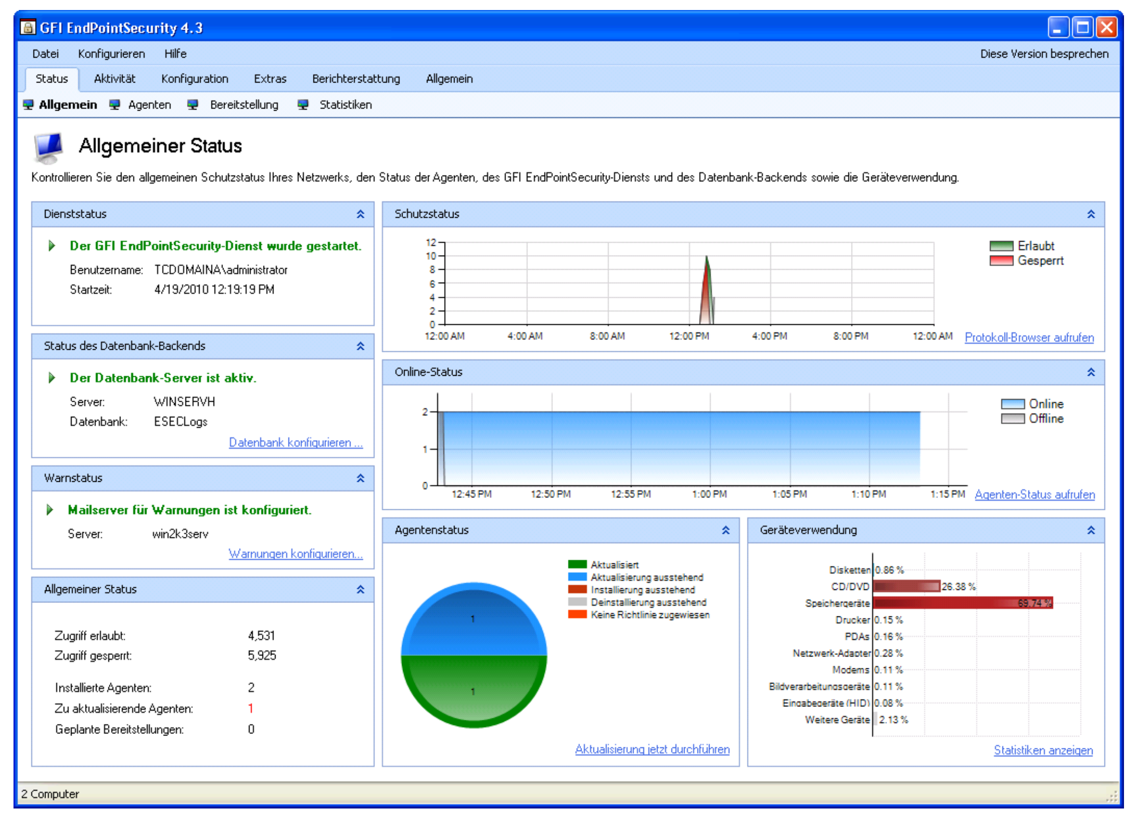
## 6.2 Allgemein

Folgende Informationen werden auf der untergeordneten Registerkarte **Allgemein** angezeigt:

» Status des GFI EndPointSecurity-Dienstes, des Datenbank-Backend-Servers und des Warnservers,

» Status der GFI EndPointSecurity-Agenten auf den kontrollierten Computern,

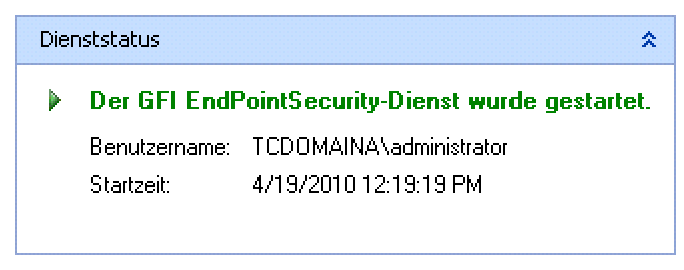
» Geräteverwendung, wie die Anzahl und Prozentsätze der gesperrten und der zugelassenen Geräte.




*Screenshot 37 - Untergeordnete Registerkarte „Allgemein“*

Klicken Sie für den Zugriff auf die untergeordnete Registerkarte **Allgemein** in der GFI EndPointSecurity-Verwaltungskonsole auf die Registerkarte **Status** ► **Allgemein**.

### 6.2.1 Dienststatus




*Screenshot 38 - Bereich „Dienststatus“*

Dieser Bereich beinhaltet:

» den Betriebsstatus der GFI EndPointSecurity-Verwaltungskonsole,

» das Benutzerkonto, unter dem der GFI EndPointSecurity-Dienst läuft,

» das Datum und die Uhrzeit des letzten Starts des Dienstes.

### 6.2.2 Datenbank-Backend-Status




*Screenshot 39 - Bereich „Datenbank-Backend-Status“*

Dieser Bereich beinhaltet:

» den Betriebsstatus des aktuell von GFI EndPointSecurity verwendeten Datenbankservers,

» den Namen oder die IP-Adresse des aktuell von GFI EndPointSecurity verwendeten Datenbankservers,

» den Namen der Datenbank, in der GFI EndPointSecurity Ereignisse archiviert.

Um die aktuellen Datenbankeinstellungen zu ändern, klicken Sie auf den Hyperlink **Datenbank konfigurieren…**. Dadurch wird der Dialog **Datenbank-Backend** geöffnet. Weitere Informationen zur Konfiguration einer zentralen Datenbank finden Sie im Kapitel Anpassen von GFI EndPointSecurity unter Konfigurieren des Datenbank-Backends.

### 6.2.3 Warnstatus




*Screenshot 40 - Bereich „Warnstatus“*

Dieser Bereich beinhaltet:

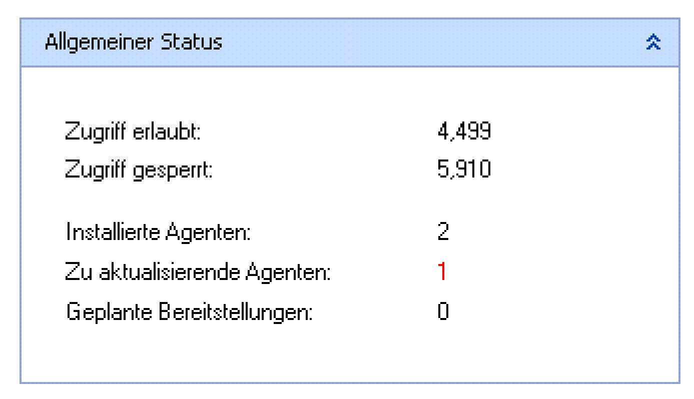
» den Betriebsstatus des aktuell von GFI EndPointSecurity verwendeten Warnservers,

» den Namen oder die IP-Adresse des aktuell von GFI EndPointSecurity verwendeten Warnservers.

Um die aktuellen Alarmeinstellungen zu ändern, klicken Sie auf den Hyperlink **Warnungen konfigurieren…**. Dadurch wird der Dialog **Warnoptionen** geöffnet. Weitere Informationen

finden Sie im Kapitel **Anpassen von GFI EndPointSecurity** unter **Konfigurieren der Warnoptionen**.

### 6.2.4 Allgemeiner Status




*Screenshot 41 - Bereich „Allgemeiner Status“*

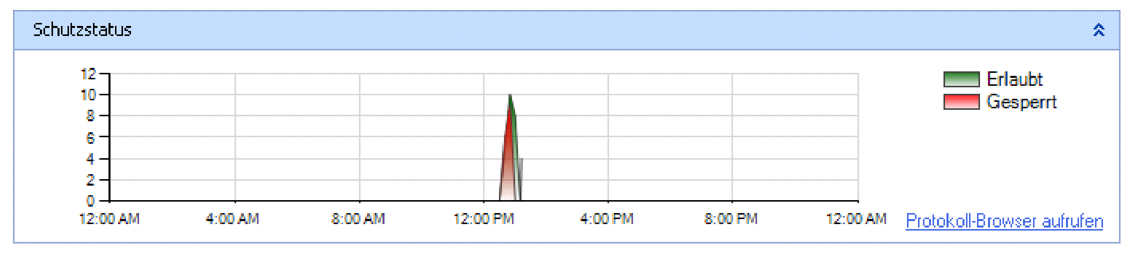


Zugriffsspezifische Werte werden als „k. A.“ angegeben. Die agentenspezifischen Werte werden in diesem Bereich auf Null gesetzt, falls kein Datenbank-Backend konfiguriert ist. Weitere Informationen zur Konfiguration einer zentralen Datenbank finden Sie im Kapitel **Anpassen von GFI EndPointSecurity** unter **Konfigurieren des Datenbank-Backends**.

Dieser Bereich enthält die kumulativen Werte zur Anzahl der:

- Benutzerzugriffe auf durch die Agenten zugelassene Geräte,
- Benutzerzugriffe auf durch die Agenten blockierte Geräte,
- auf Netzwerkcomputern installierten Agenten,
- zu aktualisierenden Agenten, darunter:
  - zu installierende Agenten,
  - zu deinstallierende Agenten,
  - zu aktualisierende Schutzrichtlinien,
- geplante Bereitstellungen, darunter:
  - zu installierende Agenten,
  - zu deinstallierende Agenten,
  - zu aktualisierende Schutzrichtlinien.

### 6.2.5 Schutzstatus




*Screenshot 42 - Bereich „Schutzstatus“*

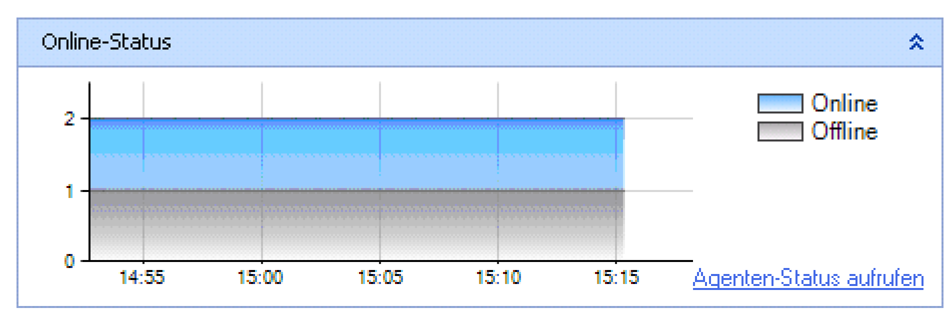


Falls kein Datenbank-Backend konfiguriert ist, wird in diesem Bereich nichts angezeigt. Weitere Informationen zur Konfiguration einer zentralen Datenbank finden Sie im Kapitel **Anpassen von GFI EndPointSecurity** unter **Konfigurieren des Datenbank-Backends**.

In diesem Bereich wird die Geräteaktivität auf Computern im Tagesverlauf anhand eines Diagramms angezeigt. Zugelassene und gesperrte Geräte werden farblich unterschieden.

Klicken Sie für eine genauere Analyse der Ereignisse zu gesperrten/zugelassenen Geräten auf den Hyperlink **Protokoll-Browser anzeigen**. Dadurch wird die untergeordnete Registerkarte **Protokoll-Browser** geöffnet. Weitere Informationen finden Sie im Kapitel **Überwachen der Geräteaktivität** unter **Untergeordnete Registerkarte „Protokoll-Browser“**.

### 6.2.6 Online-Status

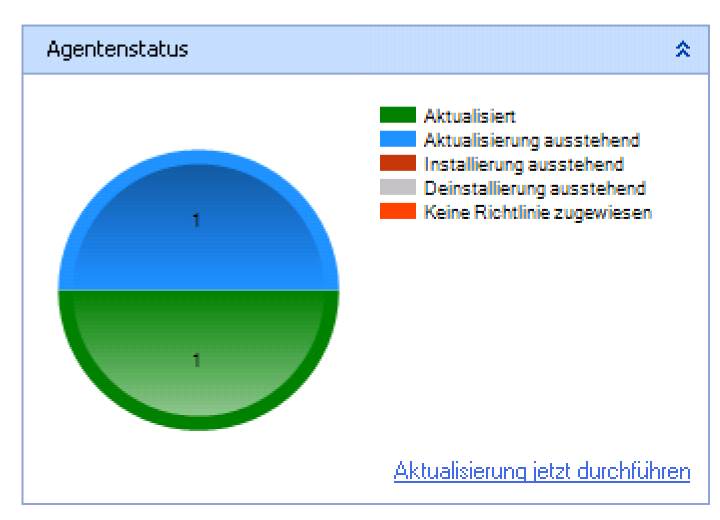



*Screenshot 43 - Bereich „Online-Status“*

In diesem Bereich wird der Status (online/offline) aller auf Computern bereitgestellten Agenten anhand eines Diagramms angezeigt.

Klicken Sie zur Anzeige von Details zum Agentenstatus auf den Hyperlink **Agentenstatus anzeigen**. Dadurch wird die untergeordnete Registerkarte **Agenten** geöffnet. Weitere Informationen finden Sie in diesem Kapitel unter **Untergeordnete Registerkarte „Agenten“**.

### 6.2.7 Agentenstatus



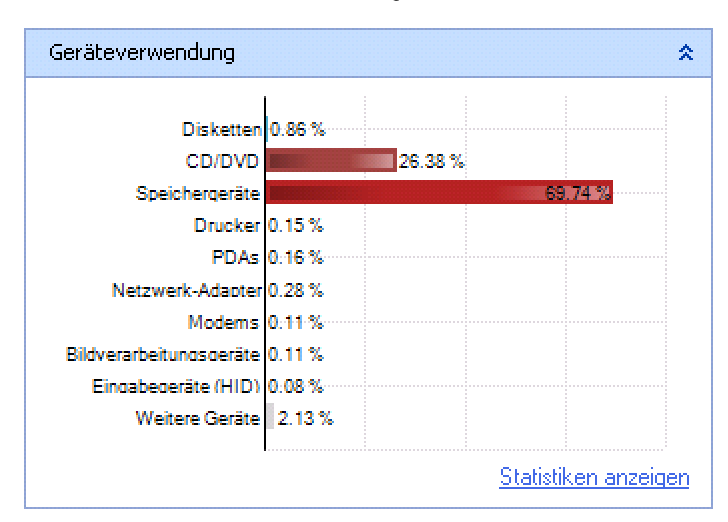

*Screenshot 44 - Bereich „Agentenstatus“*

Dieser Bereich informiert anhand eines Diagramms über die Anzahl der Agenten, die momentan:

- bereitgestellt und mit der Schutzrichtlinie synchron sind,
- bereitgestellt sind, aber durch die Änderung der Schutzrichtlinie aktualisiert werden müssen,
- auf zu kontrollierenden Computern installiert werden müssen,
- auf kontrollierten Computern deinstalliert werden müssen,
- nicht durch eine Schutzrichtlinie geschützt werden.

Klicken Sie zur Deinstallation eines Agenten auf den Hyperlink **Aktualisierung jetzt durchführen**. Dadurch wird der Dialog **Computer für Bereitstellung auswählen** geöffnet. Wählen Sie dort die gewünschten kontrollierten Computer aus, und klicken Sie anschließend auf **OK**.

### 6.2.8 Geräteverwendung




*Screenshot 45 - Bereich „Geräteverwendung“*



Falls kein Datenbank-Backend konfiguriert ist, wird in diesem Bereich nichts angezeigt. Weitere Informationen zur Konfiguration einer zentralen Datenbank finden Sie im Kapitel **Anpassen von GFI EndPointSecurity** unter **Konfigurieren des Datenbank-Backends**.

In diesem Bereich wird in einem Diagramm der von den Agenten protokollierte Prozentsatz der Benutzerzugriffe pro Gerätekategorie im Vergleich zur Gesamtzahl der Gerätezugriffe angezeigt. Benutzerzugriffe auf Geräte beziehen sich sowohl auf zugängliche als auch blockierte Geräte.

Um eine statistische Übersicht zur Gerätverwendung mit der Anzahl der Gerätetypen und Schnittstellen anzuzeigen, die für entweder einen einzelnen oder alle Computer zugänglich oder blockiert sind, klicken Sie auf den Hyperlink **Statistik anzeigen**. Dadurch wird die untergeordnete Registerkarte **Statistik** geöffnet. Weitere Informationen finden Sie im Kapitel **Überwachen der Geräteaktivität** unter **Untergeordnete Registerkarte „Statistik“**.

## 6.3 Agenten

Über die untergeordnete Registerkarte **Agenten** können Sie den Status aller Bereitstellungsvorgänge auf Ihren Netzwerkcomputern bestimmen. Folgende Informationen werden für jeden Computer angezeigt:

» Name des kontrollierten Computers und zugewiesene Schutzrichtlinie,

» Status aller aktuell bereitgestellten und aktualisierten GFI EndPointSecurity-Agenten oder die noch bereitzustellenden Agenten,

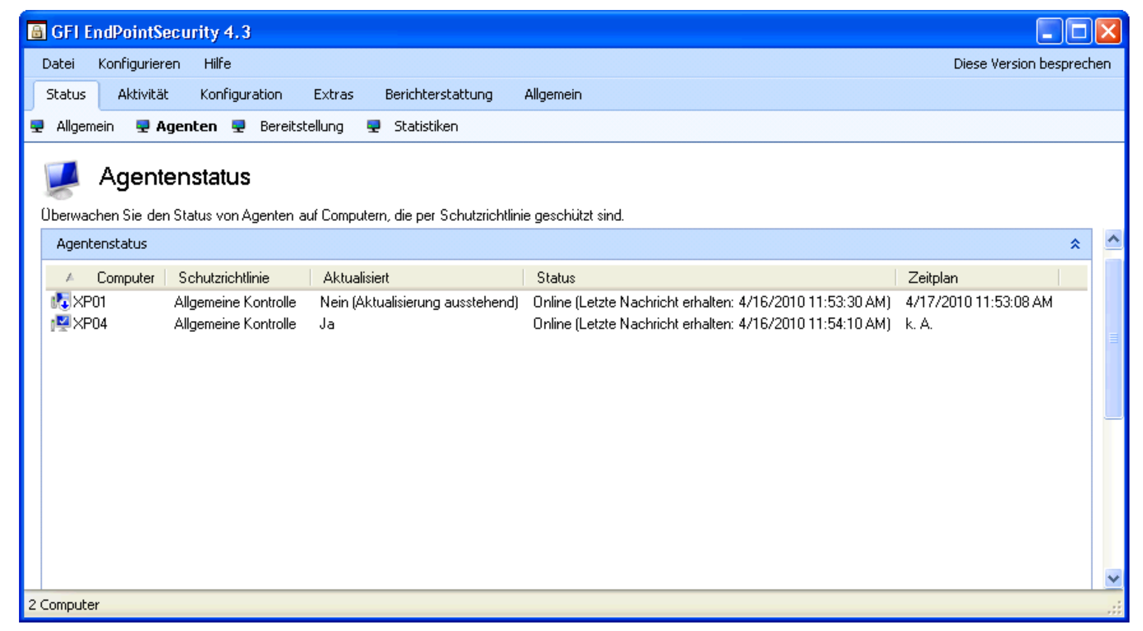
» Status der kontrollierten Computer (online/offline).



Falls ein zu kontrollierender Computer offline ist, erfolgt eine Stunde später automatisch ein erneuter Versuch. GFI EndPointSecurity versucht die Richtlinie so lange jede Stunde bereitzustellen, bis der zu kontrollierende Computer wieder online ist.



Jeder Agent sendet regelmäßig seinen Onlinestatus an die Hauptinstallation von GFI EndPointSecurity. Falls diese Daten nicht von der Hauptinstallation empfangen werden, wird der Agent als offline angesehen.




*Screenshot 46 - Untergeordnete Registerkarte „Agenten“*

Klicken Sie für den Zugriff auf die untergeordnete Registerkarte **Agenten** in der GFI EndPointSecurity-Verwaltungskonsole auf die Registerkarte **Status** ► **Agenten**.

So stellen Sie ausstehende Agenten bereit:

1. Wählen Sie einen oder mehrere Computer aus dem Abschnitt **Agentenstatus** aus.

2. Klicken Sie mit der rechten Maustaste auf die ausgewählten Computer, und wählen Sie **Ausgewählte/n Agenten bereitstellen** oder **Bereitstellungszeitplan für ausgewählte/n Agenten festlegen...**. Klicken Sie anschließend auf **OK**.

## 6.4 Bereitstellung

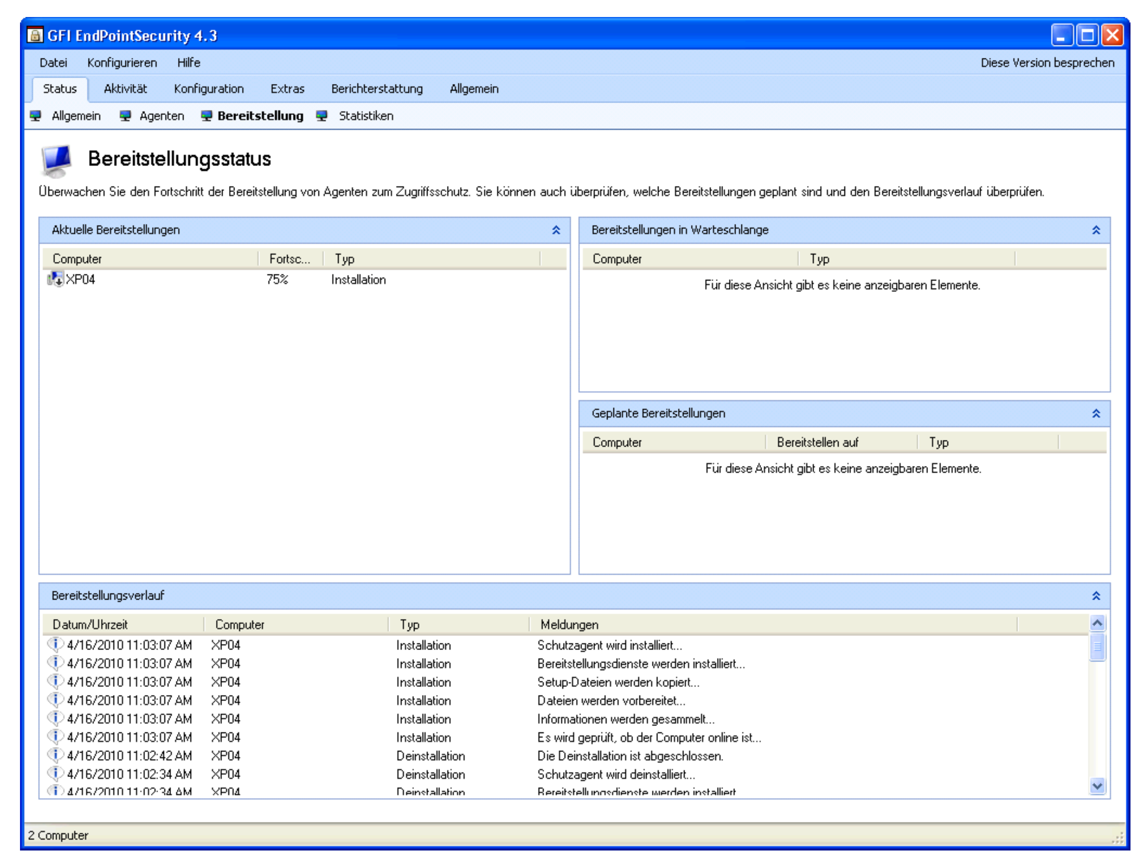
Folgende Informationen werden auf der untergeordneten Registerkarte **Bereitstellung** angezeigt:

» Aktuelle Bereitstellungsabläufe,

» Bereitstellungen in Warteschlange,

» Geplante Bereitstellungen,

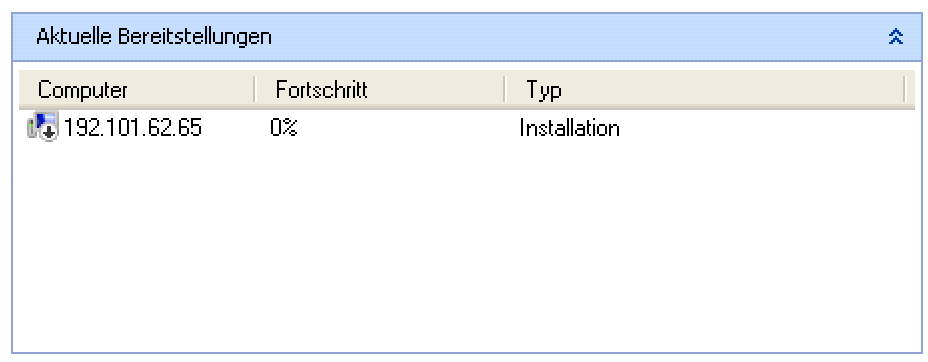
» Bereitstellungsverlauf.




*Screenshot 47 - Untergeordnete Registerkarte „Bereitstellung“*

Klicken Sie für den Zugriff auf die untergeordnete Registerkarte **Bereitstellung** in der GFI EndPointSecurity-Verwaltungskonsole auf die Registerkarte **Status** ► **Bereitstellung**.

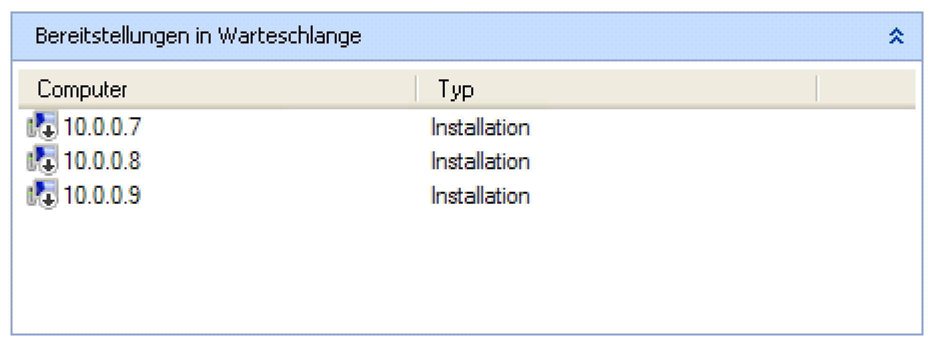
## 6.4.1 Aktive Bereitstellungen




*Screenshot 48 - Bereich „Aktive Bereitstellungen“*

In diesem Bereich werden alle aktuell aktiven Bereitstellungen angezeigt. Sie erhalten Informationen zum Namen des Computers sowie zum Fortschritt und Typ der Bereitstellung (d. h. ob es sich um eine Installation, Deinstallation oder Aktualisierung handelt).

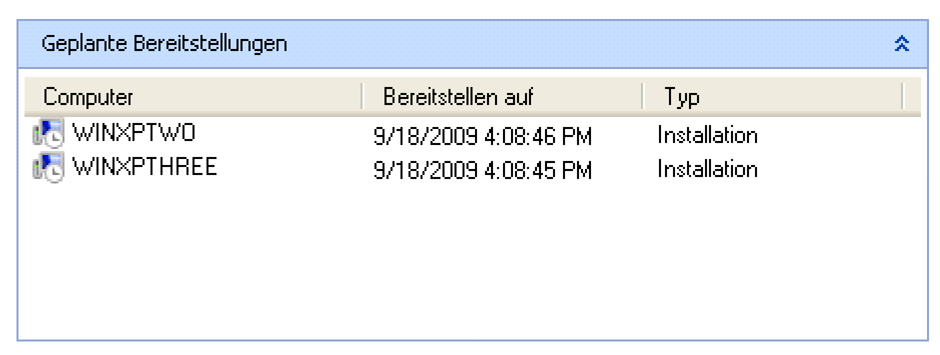
## 6.4.2 Bereitstellungen in Warteschlange




*Screenshot 49 - Bereich „Bereitstellungen in Warteschlange“*

In diesem Bereich werden alle ausstehenden Bereitstellungen angezeigt, die sich in der Warteschlange befinden. Sie erhalten Informationen zum Namen des Computers und zum Bereitstellungstyp.

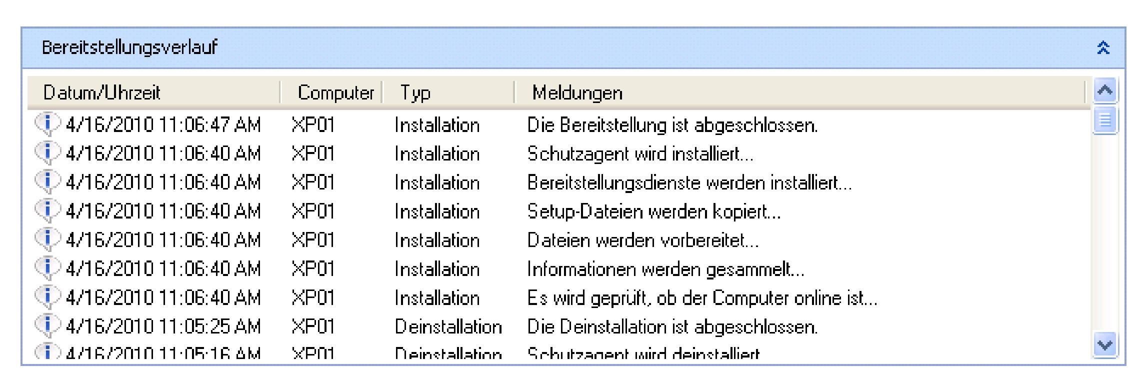
## 6.4.3 Geplante Bereitstellungen




*Screenshot 50 - Bereich „Geplante Bereitstellungen“*

In diesem Bereich werden alle geplanten Bereitstellungen angezeigt. Sie erhalten Informationen zum Namen des Computers, zur geplanten Zeit und zum Bereitstellungstyp.

## 6.4.4 Bereitstellungsverlauf




*Screenshot 51 - Bereich „Bereitstellungsverlauf“*

In diesem Bereich sind alle Stadien aller von GFI EndPointSecurity durchgeführten Agenten- bzw. Schutzrichtlinienbereitstellungen anhand eines Audit-Trails aufgeführt. Die bereitgestellten Informationen beinhalten einen Zeitstempel für jeden Protokolleintrag, Computernamen, Bereitstellungstyp, Fehler und während der Bereitstellung generierte Informationenbenachrichtigung.

Weitere Informationen zu Fehlermeldungen, die während der Bereitstellung von Agenten und Schutzrichtlinien auftreten können, finden Sie im Kapitel Anhang 1 - Bereitstellungsfehlermeldungen dieses Handbuchs.

Um angezeigte Protokolleinträge zu entfernen, klicken Sie im Bereich **Bereitstellungsverlauf** auf **Alle Nachrichten löschen**.

## 6.5 Statistik

Weitere Informationen zur untergeordneten Registerkarte **Statistik** finden Sie im Kapitel **Überwachen der Geräteaktivität** unter **Untergeordnete Registerkarte „Statistik“**.

# 7 Berichterstattung

Das GFI EndPointSecurity ReportPack ist ein vollständig integrierbares, umfassendes Reporting-Modul für GFI EndPointSecurity. Mit dem ReportPack können die von GFI EndPointSecurity erfassten Daten automatisch nach Zeitplan in Form von aussagekräftigen IT- und Management-Berichten ausgegeben werden. So bleiben Sie über mit dem Netzwerk verbundene Geräte informiert und erhalten unter anderem Trend-Daten zur Verwendung von Geräten je Rechner oder Benutzer. Sogar über mobile Hardware ausgetauschte Dokumente werden inklusive ihrer Dateinamen angezeigt.

Um Berichte erstellen zu können, müssen Sie das Add-On zum GFI EndPointSecurity ReportPack herunterladen und installieren.

Weitere Informationen zum GFI EndPointSecurity ReportPack und GFI ReportCenter finden Sie entweder:

1. In der GFI EndPointSecurity-Verwaltungskonsole auf der Registerkarte **Berichterstattung**.

2. Im linken Bereich unter **GFI EndPointSecurity ReportPack** oder **GFI ReportCenter.**

oder

» GFI EndPointSecurity ReportPack:

  **http://www.gfi.com/endpointsecurity/esecreportpack.htm**

» GFI ReportCenter:

  **http://www.gfi.com/page/4713/gfirc**

# 8 Erkennen von Geräten

## 8.1 Einführung

GFI EndPointSecurity gibt Ihnen die Möglichkeit, Endgeräte im Unternehmensnetzwerk schnell und transparent aufzuspüren und alle Geräte, die an den kontrollierten Computern angeschlossen sind oder waren, zu melden. Diese werden anschließend mit detaillierten Informationen angezeigt.



Ein erkannter Computer kann jeder Computer im Netzwerk sein und muss nicht unter eine Schutzrichtlinie von GFI EndPointSecurity fallen.



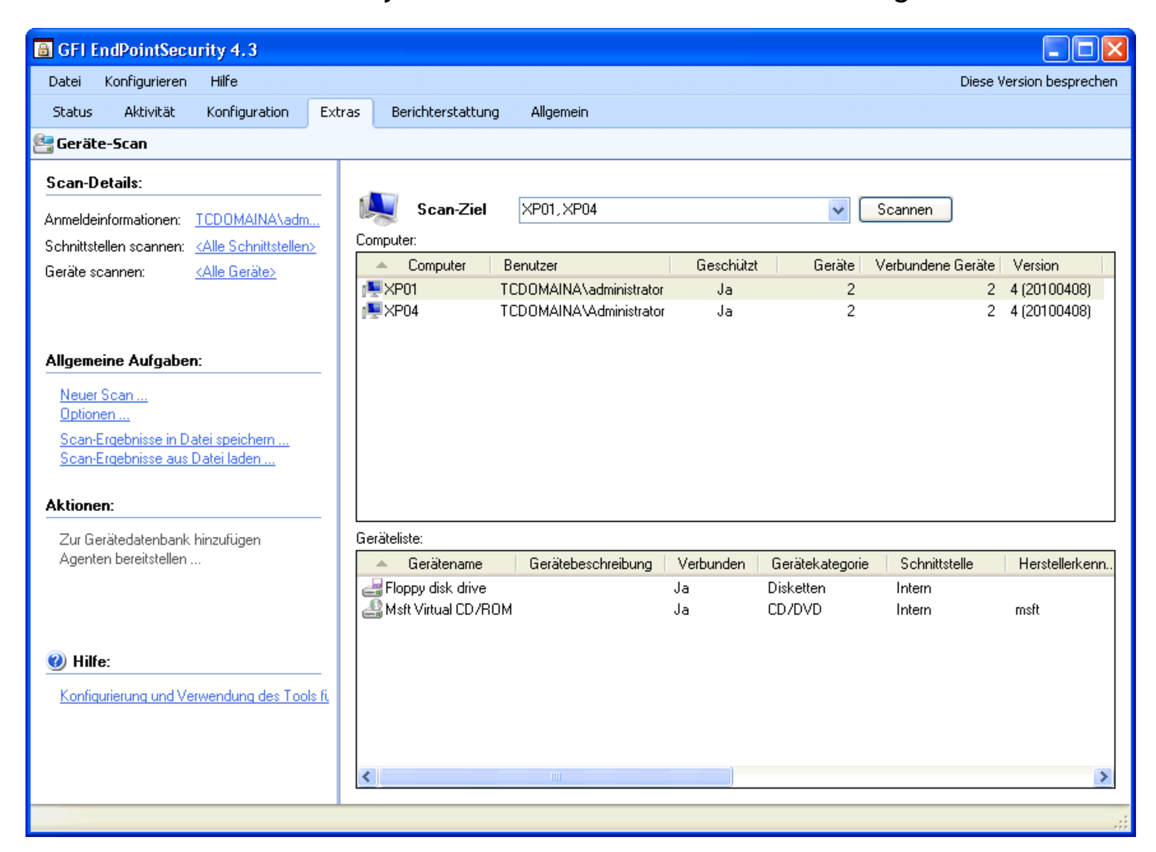
Der Geräte-Scan muss unter einem Konto mit administrativen Berechtigungen für den zu überprüfenden Computer durchgeführt werden.

## 8.2 Geräte-Scan

Verwenden Sie die untergeordnete Registerkarte **Geräte-Scan**, um Computer zu scannen und angeschlossene Geräte zu erkennen.

Standardmäßig geschieht Folgendes:

» GFI EndPointSecurity scannt alle unterstützten Gerätekategorien und Schnittstellen.



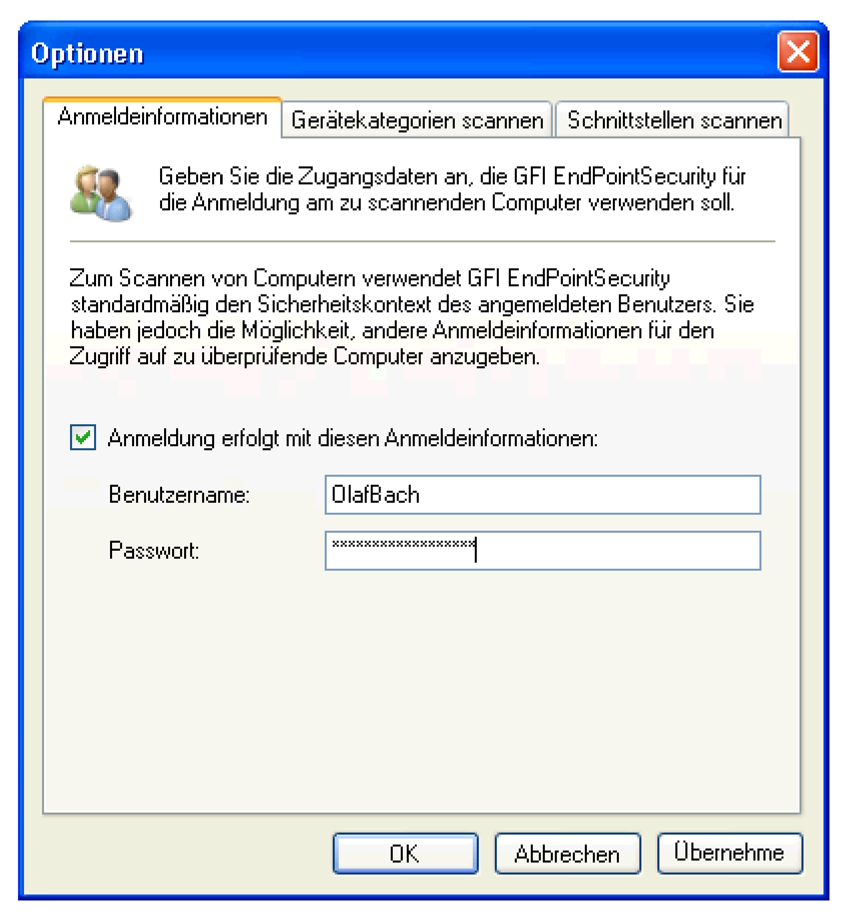

*Screenshot 52 - Untergeordnete Registerkarte „Geräte-Scan“*

### 8.2.1 Durchführen eines Geräte-Scans

So führen Sie einen Geräte-Scan durch:

1. Klicken Sie in der GFI EndPointSecurity-Verwaltungskonsole auf die Registerkarte **Extras**.
2. Klicken Sie auf die untergeordnete Registerkarte **Geräte-Scan**.

3. Klicken Sie im linken Bereich im Abschnitt **Scan Details** auf den Hyperlink **Anmeldeinformationen.**



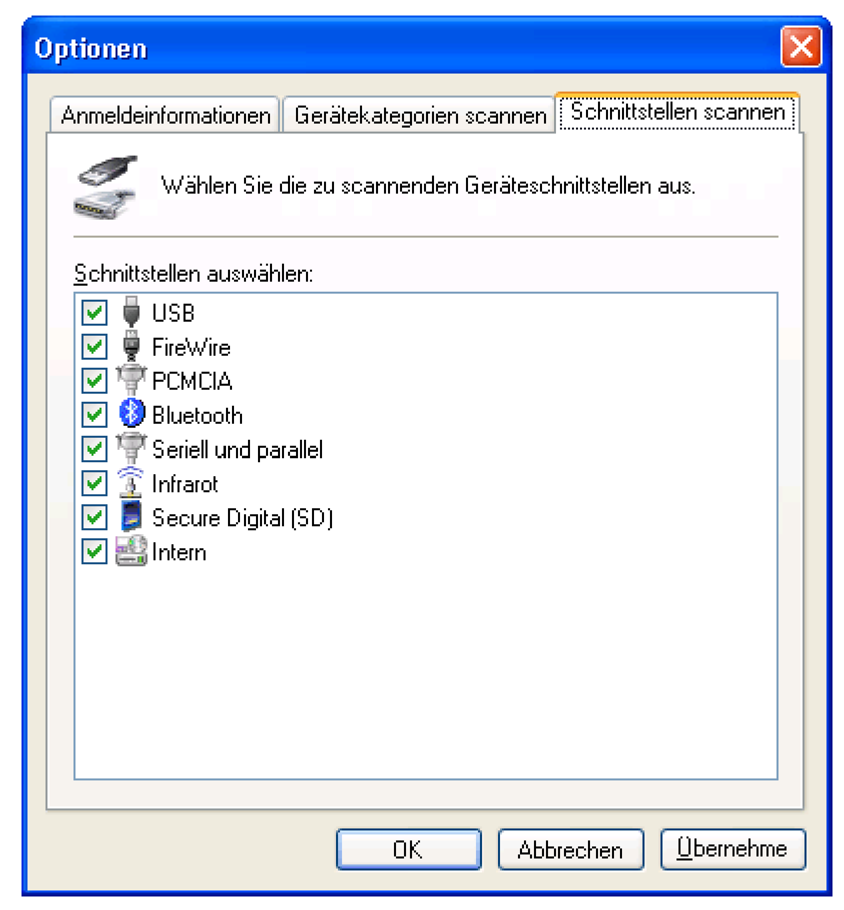

*Screenshot 53 - Optionen der Registerkarte „Anmeldeinformationen“*

4. Aktivieren Sie im Dialog **Optionen** das Kontrollkästchen **Anmeldung erfolgt mit diesen Anmeldeinformationen**, und geben Sie die Anmeldeinformationen ein, die GFI EndPointSecurity zur Verbindung mit den zu scannenden Computer verwenden soll. Klicken Sie anschließend auf **OK**.



GFI EndPointSecurity verwendet standardmäßig die Anmeldeinformationen des aktuell angemeldeten Benutzers, unter dem die GFI EndPointSecurity ausgeführt wird.

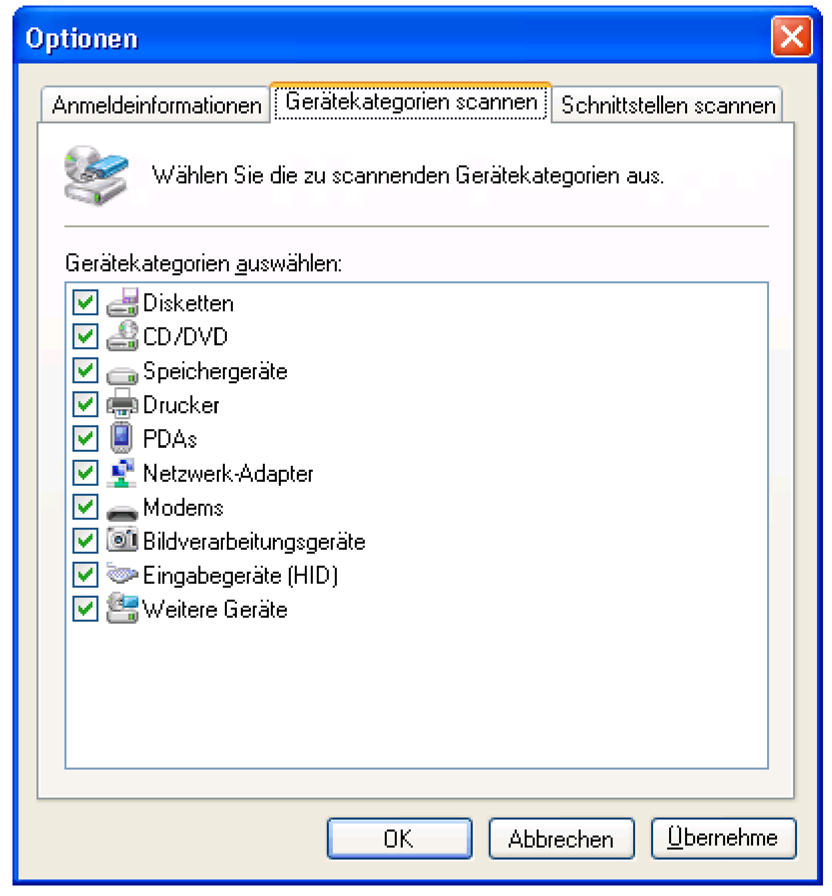
5. Klicken Sie im linken Bereich im Abschnitt **Scan-Details** auf den Hyperlink **Ports scannen.**




*Screenshot 54 - Optionen für Registerkarte „Ports scannen"*

6. Aktivieren bzw. deaktivieren Sie im Dialog **Optionen** die zu scannenden Schnittstellen, die von Geräten zur Verbindung mit den kontrollierten Computern verwendet werden könnten. Klicken Sie anschließend auf **OK.**

7. Klicken Sie im linken Bereich im Abschnitt **Scan-Details** auf den Hyperlink **Geräte scannen**.




*Screenshot 55 - Optionen für Registerkarte „Geräte scannen“*

8. Aktivieren bzw. deaktivieren Sie im Dialog **Optionen** die zu scannenden Gerätekategorien, deren untergeordnete Geräte mit den kontrollierten Computern verbunden sein könnten. Klicken Sie anschließend auf **OK**.

9. So legen Sie zu scannende Computer fest:

» Option 1: Geben Sie im rechten Bereich in das Textfeld **Scan-Ziel** den Computernamen oder die IP-Adresse des zu scannenden Computers ein. Klicken Sie anschließend auf **Scannen**, um die Geräteerkennung zu starten.

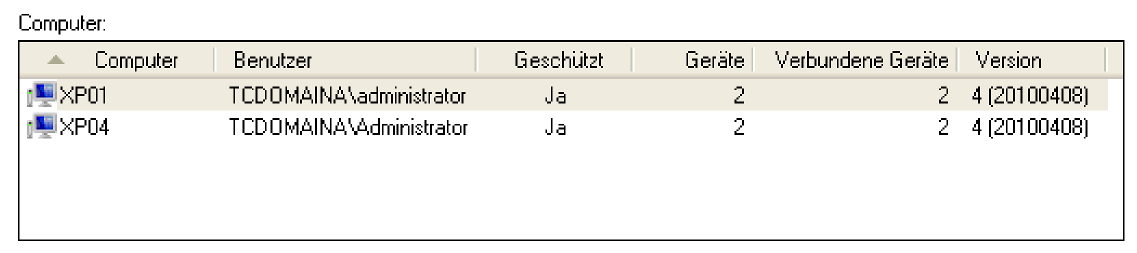
» Option 2: Klicken Sie im linken Bereich auf den Hyperlink **Neuer Scan**, und geben Sie die gewünschten zu scannenden Computer ein. Die verfügbaren Optionen sind einzelne Computer, ein Computerbereich oder eine Liste von Computern.

### 8.2.2 Ergebnisse des Geräte-Scans

Ergebnisse des Geräte-Scans werden in zwei Abschnitte unterteilt:

» Computer

» Geräteliste


Computer:

| Computer | Benutzer | Geschützt | Geräte | Verbundene Geräte | Version |
|---|---|---|---|---|---|
| XP01 | TCDOMAINA\administrator | Ja | 2 | 2 | 4 (20100408) |
| XP04 | TCDOMAINA\Administrator | Ja | 2 | 2 | 4 (20100408) |

*Screenshot 56 - Bereich „Computer“*

#### *Computer*

In diesem Bereich wird eine Zusammenfassung der Ergebnisse des Geräte-Scans für jeden gescannten Computer angezeigt. Folgende Informationen werden angezeigt:

- Computername / IP-Adresse,
- Aktuell angemeldeter Benutzer,
- Schutzstatus, d. h. ob der Computer unter eine Schutzrichtlinie von GFI EndPointSecurity fällt,
- Gesamtzahl aktuell und zuvor verbundener Geräte,
- Anzahl aktuell verbundener Geräte.

Gehört ein gescannter Computer zu keiner Schutzrichtlinie von GFI EndPointSecurity, können Sie wählen, ob er einer Richtlinie zugewiesen werden soll. Führen Sie hierfür folgende Schritte durch:

1. Klicken Sie in der Spalte **Computer** mit der rechten Maustaste auf den gewünschten Computernamen / die gewünschte IP-Adresse.

2. Wählen Sie **Agenten bereitstellen…**.

3. Wählen Sie die bereitzustellende Schutzrichtlinie aus. Klicken Sie um Fortzufahren auf **Weiter** und zum Start der Bereitstellung auf **Fertig stellen**.

### *Geräteliste*

In diesem Bereich wird eine detaillierte Liste der erkannten Geräte für jeden gescannten Computer angezeigt. Folgende Informationen werden angezeigt:

- Gerätename, Beschreibung und Kategorie
- Schnittstelle
- Verbindungsstatus, d. h. ob das Gerät aktuell angeschlossen ist.

Geräteliste:

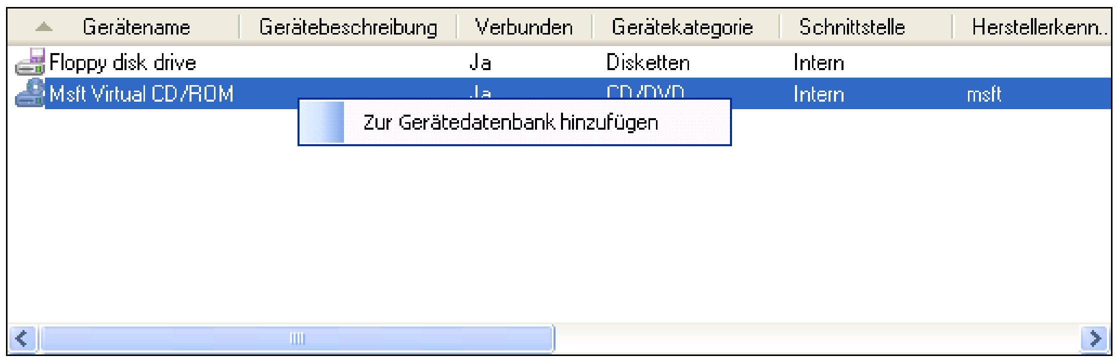



*Screenshot 57 - Bereich „Geräteliste“*

## 8.2.3 Hinzufügen von erkannten Geräten in die Gerätedatenbank

Unter **Geräteliste** können Sie ein oder mehrere erkannte Geräte auswählen und diese der Gerätedatenbank hinzufügen. Diese Geräte werden dann aus dieser Datenbank abgefragt, wenn GFI EndPointSecurity für die Blacklist- und Whitelist-Funktion die momentan an die kontrollierten Computer angeschlossenen Geräte auflistet. Weitere Informationen zur Blacklist- und Whitelist-Funktion finden Sie im Kapitel Anpassen von Schutzrichtlinien unter Konfigurieren der Geräte-Blacklist oder Konfigurieren der Geräte-Whitelist.




*Screenshot 58 - Bereich „Geräteliste“ - Hinzufügen von Geräten in die Gerätedatenbank*

So fügen Sie Geräte der Gerätedatenbank hinzu:

1. Wählen Sie im Abschnitt **Geräteliste** ein oder mehrere Geräte aus, die der Gerätedatenbank hinzugefügt werden sollen.

2. Klicken Sie mit der rechten Maustaste auf die ausgewählten Geräte, wählen Sie **Zur Gerätedatenbank hinzufügen**, und klicken Sie auf **OK**.

# 9 Anpassen von Schutzrichtlinien

## 9.1 Einführung

Alle Schutzrichtlinien innerhalb von GFI EndPointSecurity sind komplett benutzerdefinierbar und können vollständig an die unternehmensspezifischen Sicherheitsrichtlinien für Gerätezugriff angepasst werden. Dies trifft auch auf die Standardrichtlinie zu, die von der automatischen Suche von GFI EndPointSecurity verwendet wird. In diesem Kapitel werden folgende Aspekte behandelt:

- Konfigurieren kontrollierter Gerätekategorien
- Konfigurieren kontrollierter Schnittstellen
- Konfigurieren von Hauptbenutzern
- Konfigurieren von Zugriffsberechtigungen für Gerätekategorien
- Konfigurieren von Zugriffsberechtigungen für Schnittstellen
- Konfigurieren von Zugriffsberechtigungen für einzelne Geräte
- Anzeigen von Zugriffsberechtigungen
- Konfigurieren von Berechtigungsprioritäten
- Konfigurieren der Geräte-Blacklist
- Konfigurieren der Geräte-Whitelist
- Konfigurieren zeitlich begrenzter Zugriffsrechte
- Konfigurieren der Dateitypfilter
- Konfigurieren der Sicherheitsverschlüsselung
- Konfigurieren der Ereignisprotokollierung
- Konfigurieren von Alarmen
- Festlegen einer Standardrichtlinie.

## 9.2 Konfigurieren kontrollierter Gerätekategorien

GFI EndPointSecurity bietet Ihnen die Möglichkeit, festzulegen, welche Gerätekategorien durch die Schutzrichtlinie kontrolliert werden sollen. Diese Konfiguration kann für jede einzelne Richtlinie erfolgen.



Nicht festgelegte Geräte sind über die von der Schutzrichtlinie kontrollierten Computer uneingeschränkt zugänglich. Dadurch kann GFI EndPointSecurity Geräte nicht überwachen oder blockieren, die in eine nicht von der Schutzrichtlinie kontrollierte Kategorie fallen.

So geben Sie die Geräte an, die durch eine bestimmte Schutzrichtlinie kontrolliert werden sollen:

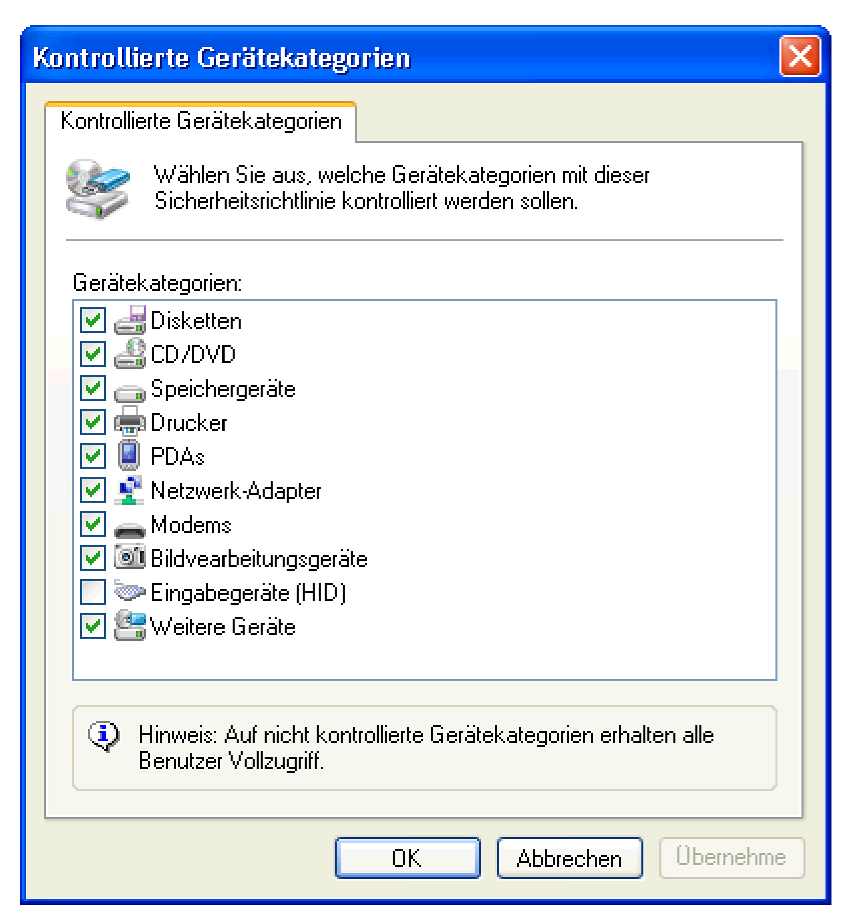
1. Klicken Sie in der GFI EndPointSecurity-Verwaltungskonsole auf die Registerkarte **Konfiguration**.

2. Klicken Sie auf die untergeordnete Registerkarte **Schutzrichtlinien**.

3. Wählen Sie im linken Bereich die zu konfigurierende Schutzrichtlinie aus.

4. Klicken Sie auf den Unterknoten **Sicherheit**.

5. Klicken Sie im linken Bereich im Abschnitt **Allgemeine Aufgaben** auf den Hyperlink **Überwachte Gerätekategorien bearbeiten....**




*Screenshot 59 - Optionen für kontrollierte Gerätekategorien*

6. Aktivieren bzw. deaktivieren Sie im Dialog **Kontrollierte Gerätekategorien** die erforderlichen Gerätekategorien, die durch die Schutzrichtlinie kontrolliert werden sollen, und klicken Sie auf **OK**.



Falls die Option **Eingabegeräte** aktiviert ist und der Zugriff verweigert wird, können Benutzer keine USB-Tastaturen oder -Mäuse verwenden, die an die durch diese Schutzrichtlinie kontrollierten Computer angeschlossen sind.

So stellen Sie Aktualisierungen für Schutzrichtlinien auf den von der Schutzrichtlinie kontrollierten Computern bereit:

1. Klicken Sie in der GFI EndPointSecurity-Verwaltungskonsole auf die Registerkarte **Konfiguration**.

2. Klicken Sie auf die untergeordnete Registerkarte **Computer**.

3. Klicken Sie im linken Bereich im Abschnitt **Allgemeine Aufgaben** auf den Hyperlink **Auf allen Computern bereitstellen....**

## 9.3 Konfigurieren kontrollierter Schnittstellen

GFI EndPointSecurity bietet Ihnen die Möglichkeit, festzulegen, welche Schnittstellen durch die Schutzrichtlinie kontrolliert werden sollen. Diese Konfiguration kann für jede einzelne Richtlinie erfolgen.



Nicht festgelegte Schnittstellen sind über die von der Schutzrichtlinie kontrollierten Computer uneingeschränkt zugänglich. Dadurch kann GFI EndPointSecurity Geräte nicht überwachen oder blockieren, die an eine nicht von der Schutzrichtlinie kontrollierte Schnittstelle angeschlossen werden.

So geben Sie die Schnittstellen an, die durch eine bestimmte Schutzrichtlinie kontrolliert werden sollen:

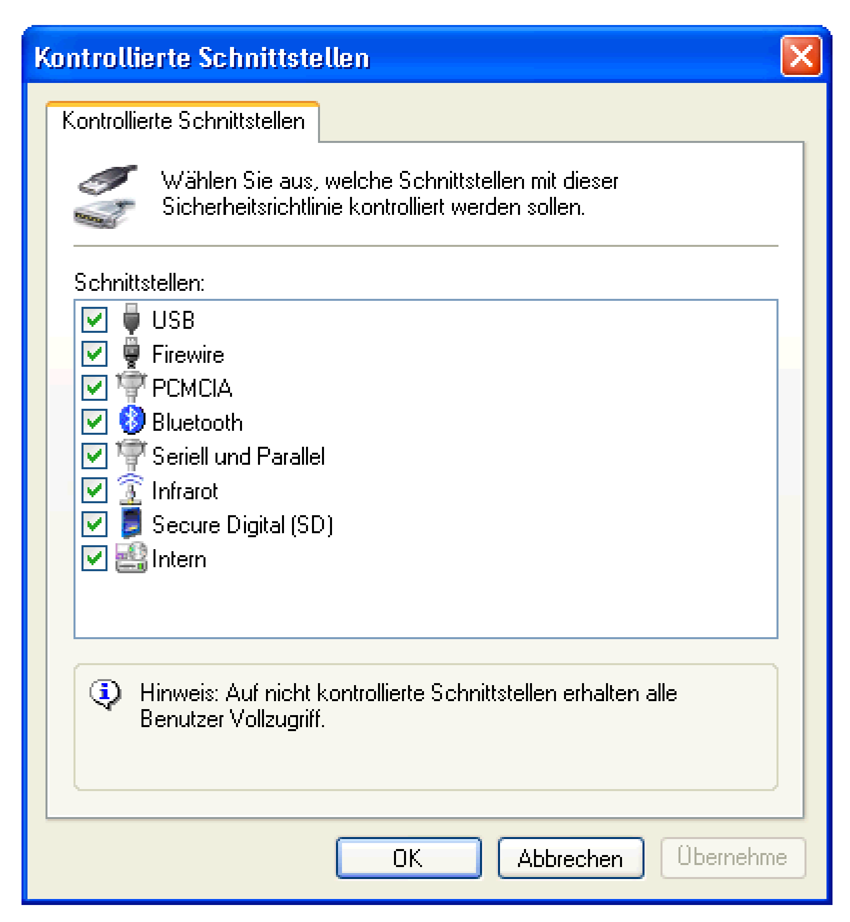
1. Klicken Sie in der GFI EndPointSecurity-Verwaltungskonsole auf die Registerkarte **Konfiguration**.

2. Klicken Sie auf die untergeordnete Registerkarte **Schutzrichtlinien**.

3. Wählen Sie im linken Bereich die zu konfigurierende Schutzrichtlinie aus.

4. Klicken Sie auf den Unterknoten **Sicherheit**.

5. Klicken Sie im linken Bereich im Abschnitt **Allgemeine Aufgaben** auf den Hyperlink **Überwachte Schnittstellen bearbeiten....**




*Screenshot 60 - Optionen für kontrollierte Schnittstellen*

6. Aktivieren bzw. deaktivieren Sie im Dialog **Kontrollierte Schnittstellen** die erforderlichen Schnittstellen, die durch die Schutzrichtlinie kontrolliert werden sollen, und klicken Sie auf **OK**.

So stellen Sie Aktualisierungen für Schutzrichtlinien auf den von der Schutzrichtlinie kontrollierten Computern bereit:

1. Klicken Sie in der GFI EndPointSecurity-Verwaltungskonsole auf die Registerkarte **Konfiguration**.

2. Klicken Sie auf die untergeordnete Registerkarte **Computer**.

3. Klicken Sie im linken Bereich im Abschnitt **Allgemeine Aufgaben** auf den Hyperlink **Auf allen Computern bereitstellen....**

## 9.4 Konfigurieren der Hauptbenutzer

GFI EndPointSecurity bietet Ihnen die Möglichkeit, Active Directory (AD)-Benutzer und/oder -Benutzergruppen, oder lokale Benutzer und/oder Benutzerschemen als Hauptbenutzer festzulegen. Hauptbenutzer besitzen automatisch vollen Zugriff auf alle Geräte, die an einem durch die Schutzrichtlinie kontrollierten Computer angeschlossen sind. Es können mehrere Hauptbenutzer für jede Schutzrichtlinie definiert werden.



**Bei der Definition von Hauptbenutzern ist große Vorsicht geboten, da für diese Benutzer sämtliche durch die jeweilige Schutzrichtlinie definierten Einschränkungen nicht gelten.**

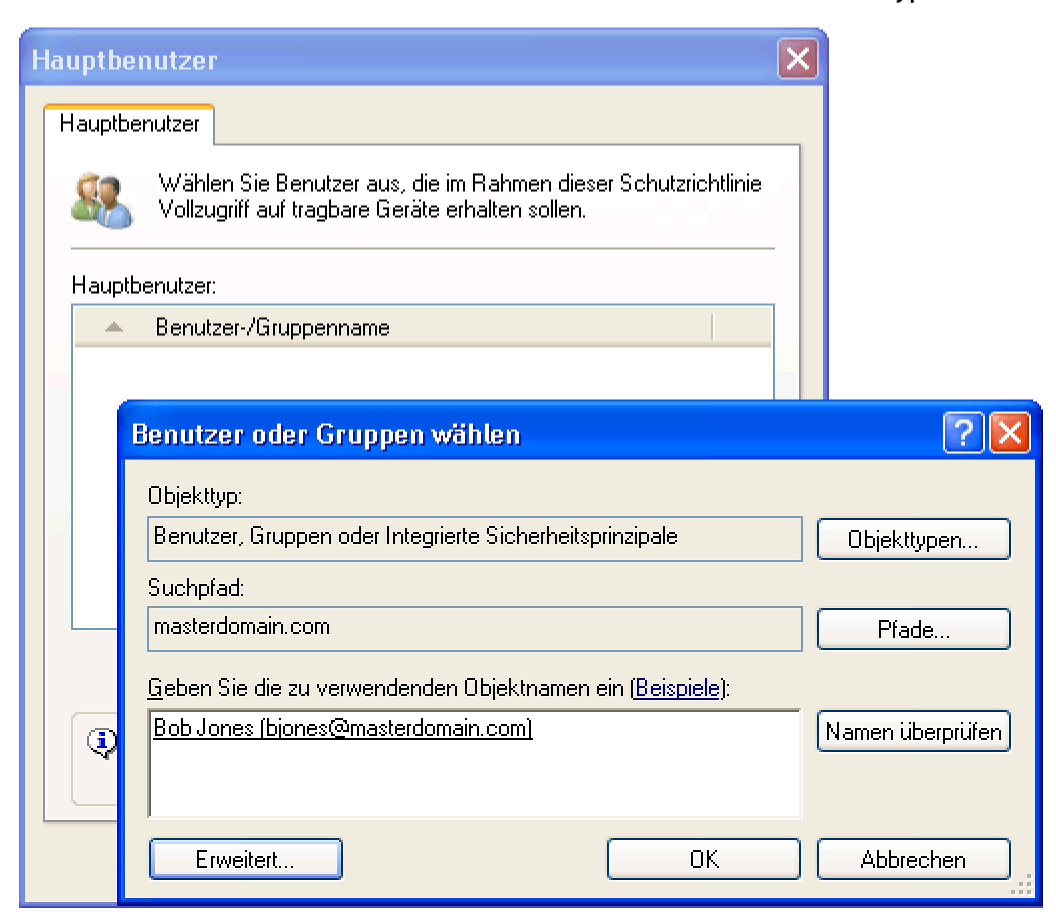
So legen Sie Hauptbenutzer für eine Schutzrichtlinie fest:

1. Klicken Sie in der GFI EndPointSecurity-Verwaltungskonsole auf die Registerkarte **Konfiguration**.

2. Klicken Sie auf die untergeordnete Registerkarte **Schutzrichtlinien**.

3. Wählen Sie im linken Bereich die Schutzrichtlinie aus, für die Sie Hauptbenutzer definieren möchten.

4. Klicken Sie im linken Bereich im Abschnitt **Sicherheit** auf den Hyperlink **Hauptbenutzer**.




*Screenshot 61 - Optionen für Hauptbenutzer*

5. Führen Sie im Dialog **Hauptbenutzer** eine der folgenden Optionen durch:

- Option 1: Klicken Sie auf **Hinzufügen**, um die Benutzer/Gruppen festzulegen, die für diese Schutzrichtlinie die Hauptbenutzer sein sollen. Klicken Sie anschließend auf **OK**.
- Option 2: Markieren Sie die Benutzer/Gruppen, die keine Hauptbenutzer mehr sein sollen, und klicken Sie auf **Entfernen**. Klicken Sie anschließend auf **OK**.

So stellen Sie Aktualisierungen für Schutzrichtlinien auf den von der Schutzrichtlinie kontrollierten Computern bereit:

1. Klicken Sie in der GFI EndPointSecurity-Verwaltungskonsole auf die Registerkarte **Konfiguration**.

2. Klicken Sie auf die untergeordnete Registerkarte **Computer**.

3. Klicken Sie im linken Bereich im Abschnitt **Allgemeine Aufgaben** auf den Hyperlink **Auf allen Computern bereitstellen...**.

## 9.5 Konfigurieren von Zugriffsberechtigungen für Gerätekategorien

GFI EndPointSecurity bietet Ihnen die Möglichkeit, Berechtigungen für Gerätekategorien den Active Directory (AD)-Benutzern und/oder -Benutzergruppen, oder lokalen Benutzern und/oder Benutzerschemen zuzuweisen. Diese Konfiguration kann für jede einzelne Richtlinie erfolgen.



Wenn eine Gerätekategorie nicht durch eine Schutzrichtlinie kontrolliert wird, ist der jeweilige Eintrag deaktiviert. Weitere Informationen zum Hinzufügen oder Entfernen der Schutzrichtlinie von Gerätekategorien finden Sie im Abschnitt Konfigurieren kontrollierter Gerätekategorien in diesem Kapitel.

So konfigurieren Sie Berechtigungen für den Zugriff auf Gerätekategorien für Benutzer innerhalb einer Schutzrichtlinie:

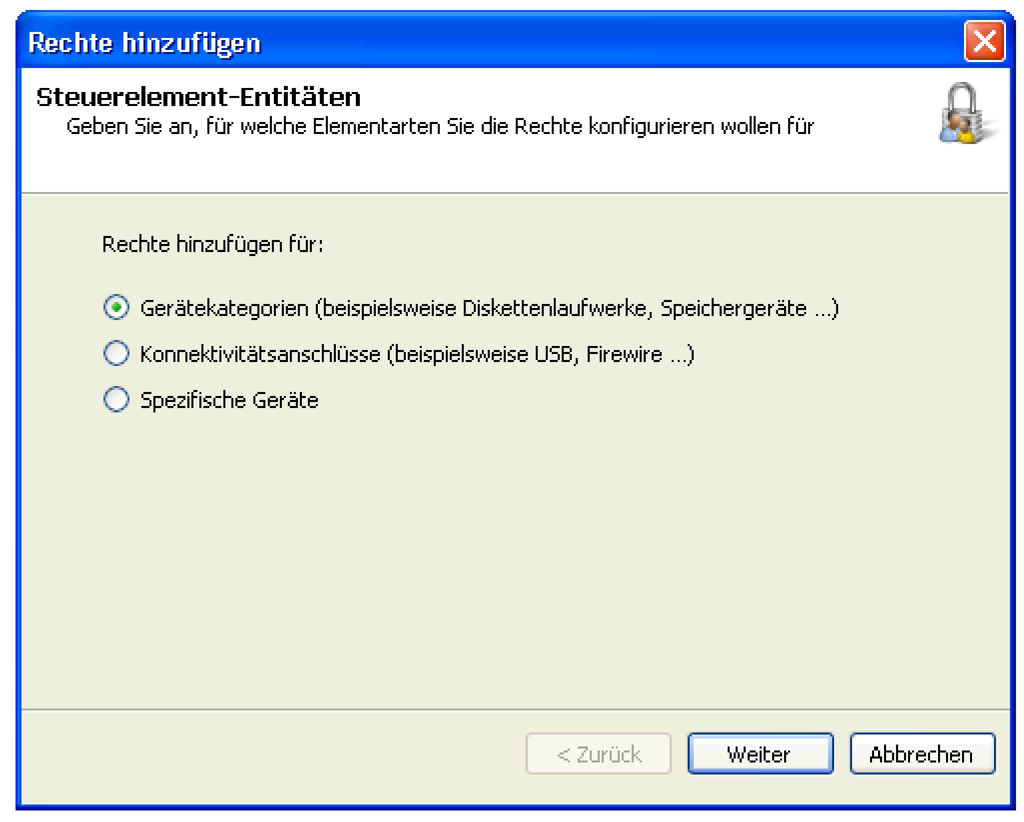
1. Klicken Sie in der GFI EndPointSecurity-Verwaltungskonsole auf die Registerkarte **Konfiguration**.

2. Klicken Sie auf die untergeordnete Registerkarte **Schutzrichtlinien**.

3. Wählen Sie im linken Bereich die zu konfigurierende Schutzrichtlinie aus.

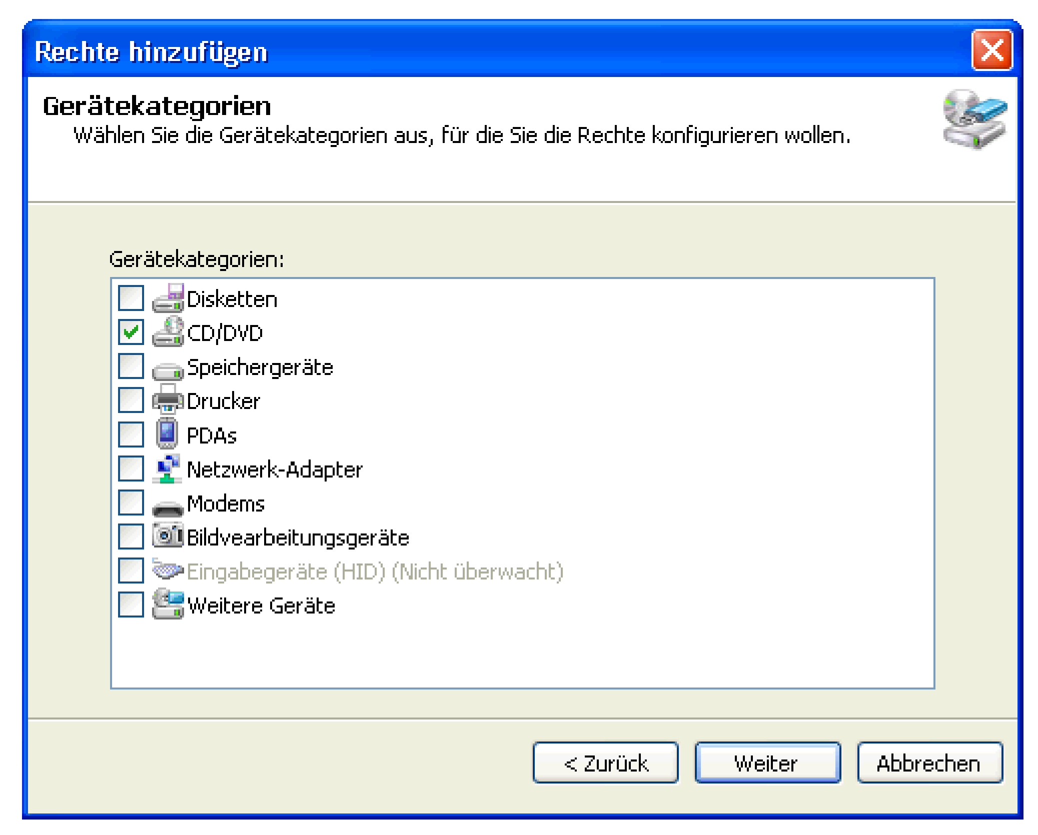
4. Klicken Sie auf den Unterknoten **Sicherheit**.

5. Klicken Sie im linken Bereich im Abschnitt **Allgemeine Aufgaben** auf den Hyperlink **Berechtigung(en) hinzufügen...**.



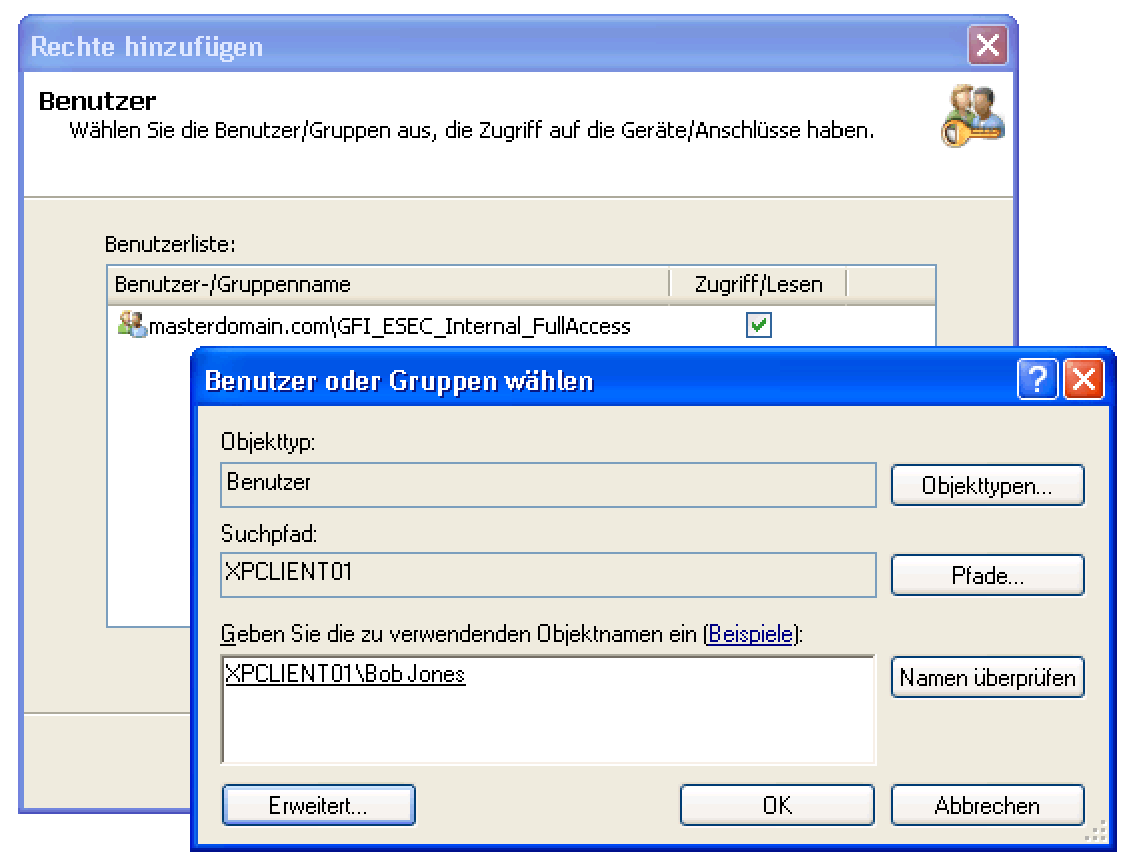

*Screenshot 62 - Optionen zum Hinzufügen von Berechtigungen - Steuerung*

6. Wählen Sie im Dialog **Berechtigungen hinzufügen** die Option **Gerätekategorien** aus, und klicken Sie zum Fortfahren auf **Weiter**.



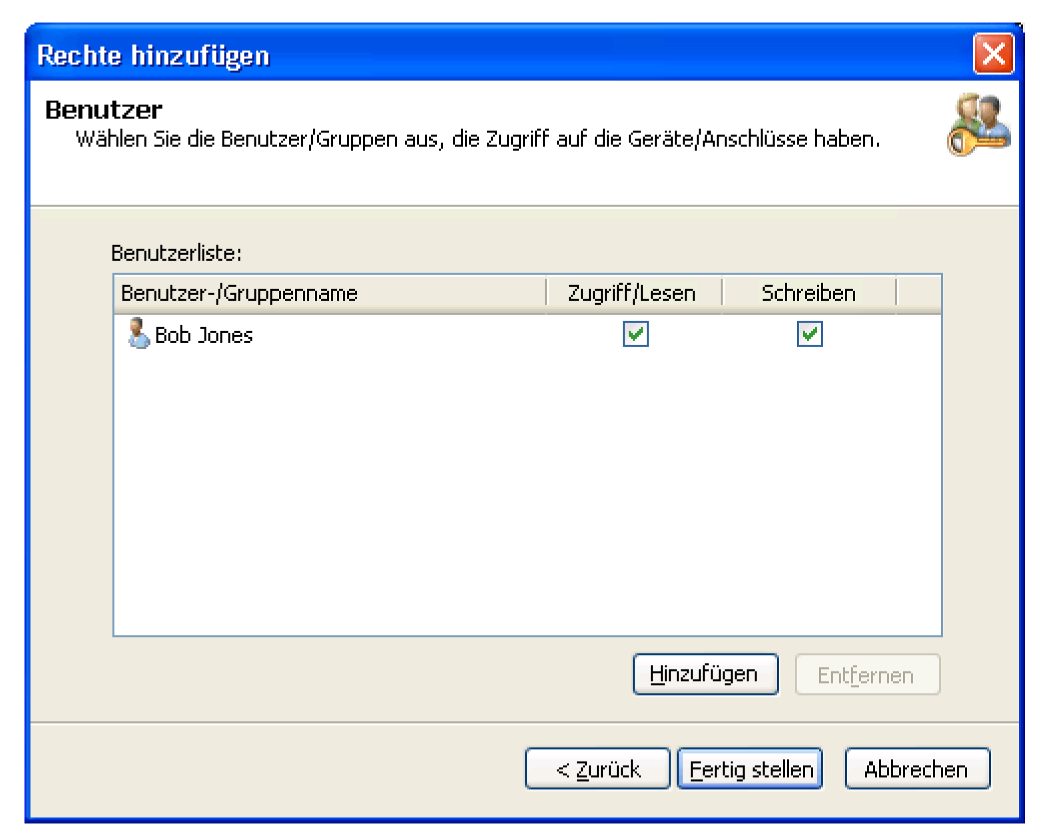

*Screenshot 63 - Optionen zum Hinzufügen von Berechtigungen - Gerätekategorien*

7. Aktivieren oder deaktivieren Sie die gewünschten Gerätekategorien, für die Berechtigungen konfiguriert werden sollen. Klicken Sie anschließend auf **Weiter**.




*Screenshot 64 - Optionen zum Hinzufügen von Berechtigungen - Benutzer*

8. Klicken Sie auf **Hinzufügen...**, um die Benutzer/Gruppen festzulegen, die auf die festgelegten Gerätekategorien in dieser Schutzrichtlinie Zugriff haben. Klicken Sie anschließend auf **OK**.




*Screenshot 65 - Optionen zum Hinzufügen von Berechtigungen - Benutzer*

9. Aktivieren oder deaktivieren Sie die Berechtigungen **Zugriff/Lesen** und **Schreiben** für festgelegte Benutzer/Gruppen. Klicken Sie anschließend auf **Fertig stellen**.

So stellen Sie Aktualisierungen für Schutzrichtlinien auf den von der Schutzrichtlinie kontrollierten Computern bereit:

1. Klicken Sie in der GFI EndPointSecurity-Verwaltungskonsole auf die Registerkarte **Konfiguration**.

2. Klicken Sie auf die untergeordnete Registerkarte **Computer**.

3. Klicken Sie im linken Bereich im Abschnitt **Allgemeine Aufgaben** auf den Hyperlink **Auf allen Computern bereitstellen....**

## 9.6 Konfigurieren von Zugriffsberechtigungen für Schnittstellen

GFI EndPointSecurity bietet Ihnen die Möglichkeit, Berechtigungen für Schnittstellen den Active Directory (AD)-Benutzern und/oder -Benutzergruppen, oder lokalen Benutzern und/oder Benutzerschemen zuzuweisen. Diese Konfiguration kann für jede einzelne Richtlinie erfolgen.



Wenn eine Schnittstelle nicht durch eine Schutzrichtlinie kontrolliert wird, ist die jeweilige Berechtigung deaktiviert. Weitere Informationen zum Hinzufügen oder Entfernen der Schutzrichtlinie von Schnittstellen finden Sie im Abschnitt Konfigurieren kontrollierter Schnittstellen in diesem Kapitel.

So konfigurieren Sie Benutzerberechtigungen für die Verwendung von Schnittstellen innerhalb einer Schutzrichtlinie:

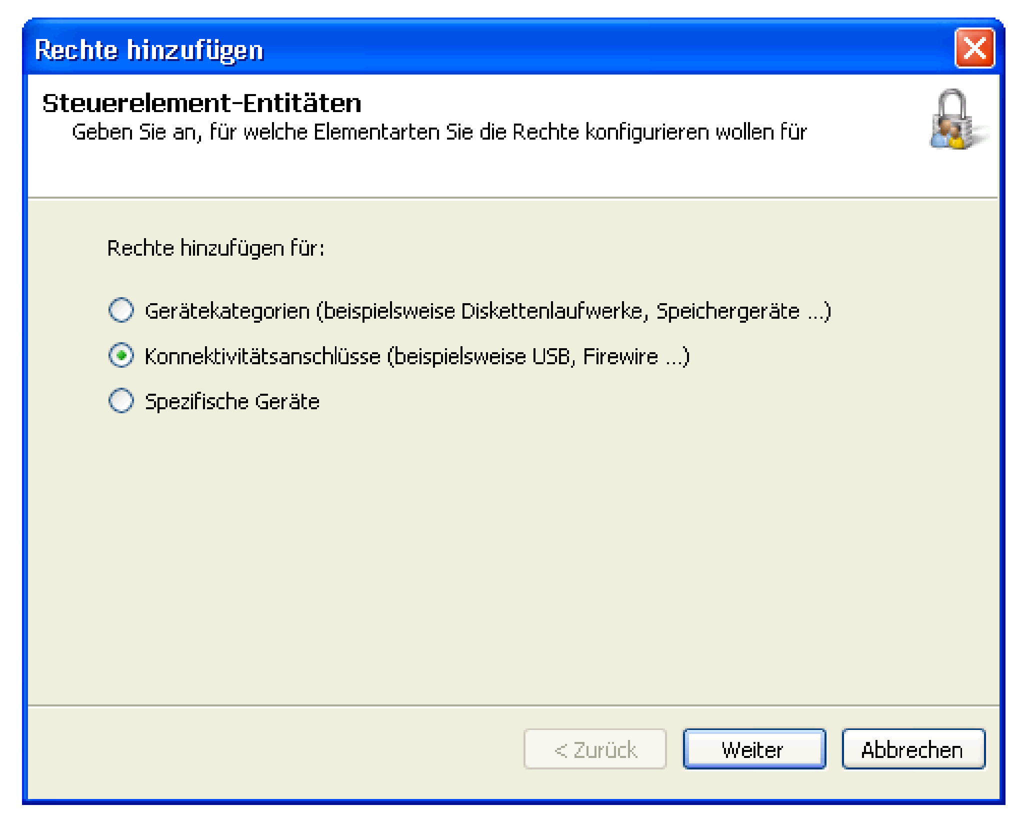
1. Klicken Sie in der GFI EndPointSecurity-Verwaltungskonsole auf die Registerkarte **Konfiguration**.

2. Klicken Sie auf die untergeordnete Registerkarte **Schutzrichtlinien**.

3. Wählen Sie im linken Bereich die zu konfigurierende Schutzrichtlinie aus.

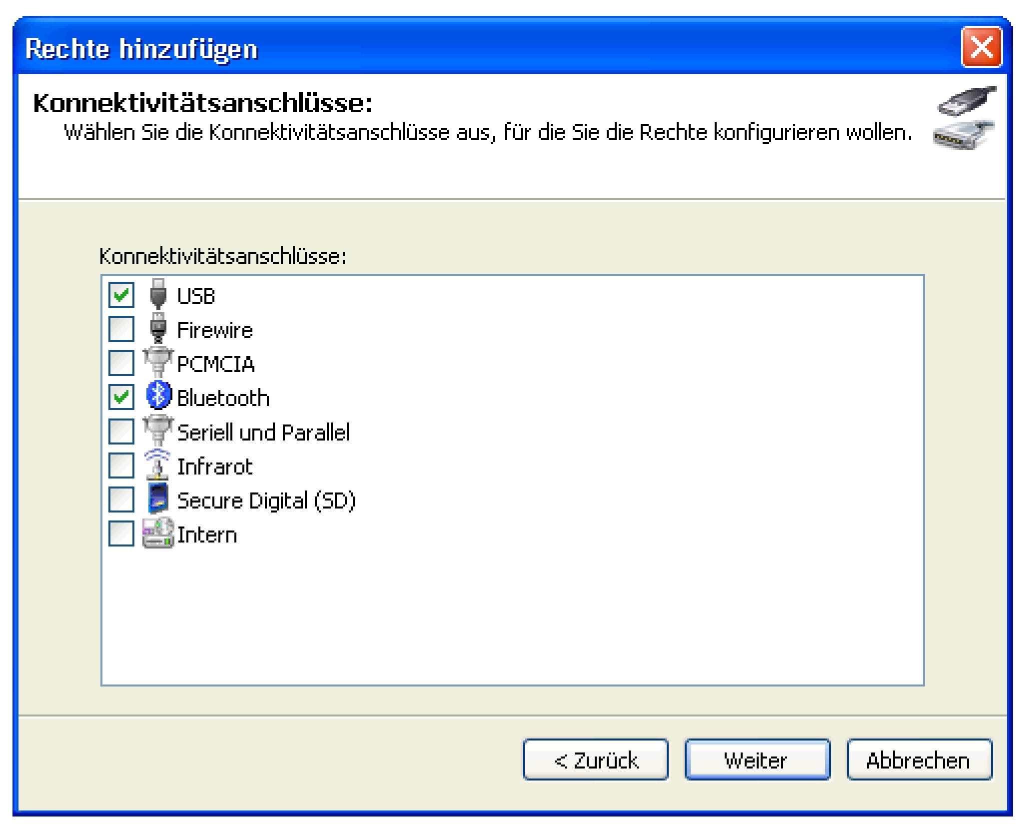
4. Klicken Sie auf den Unterknoten **Sicherheit**.

5. Klicken Sie im linken Bereich im Abschnitt **Allgemeine Aufgaben** auf den Hyperlink **Berechtigung(en) hinzufügen....**



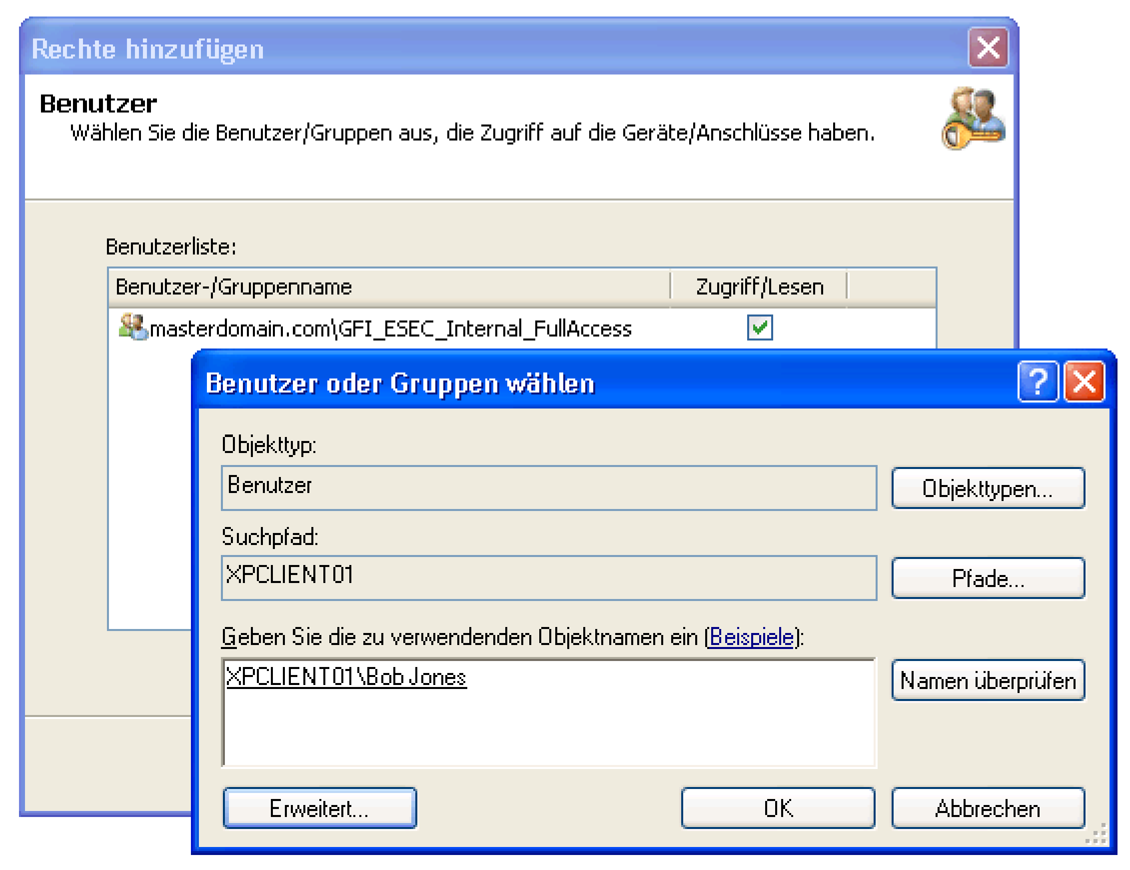

*Screenshot 66 - Optionen zum Hinzufügen von Berechtigungen - Steuerung*

6. Wählen Sie im Dialog **Berechtigungen hinzufügen** die Option **Schnittstellen**, und klicken Sie zum Fortfahren auf **Weiter**.



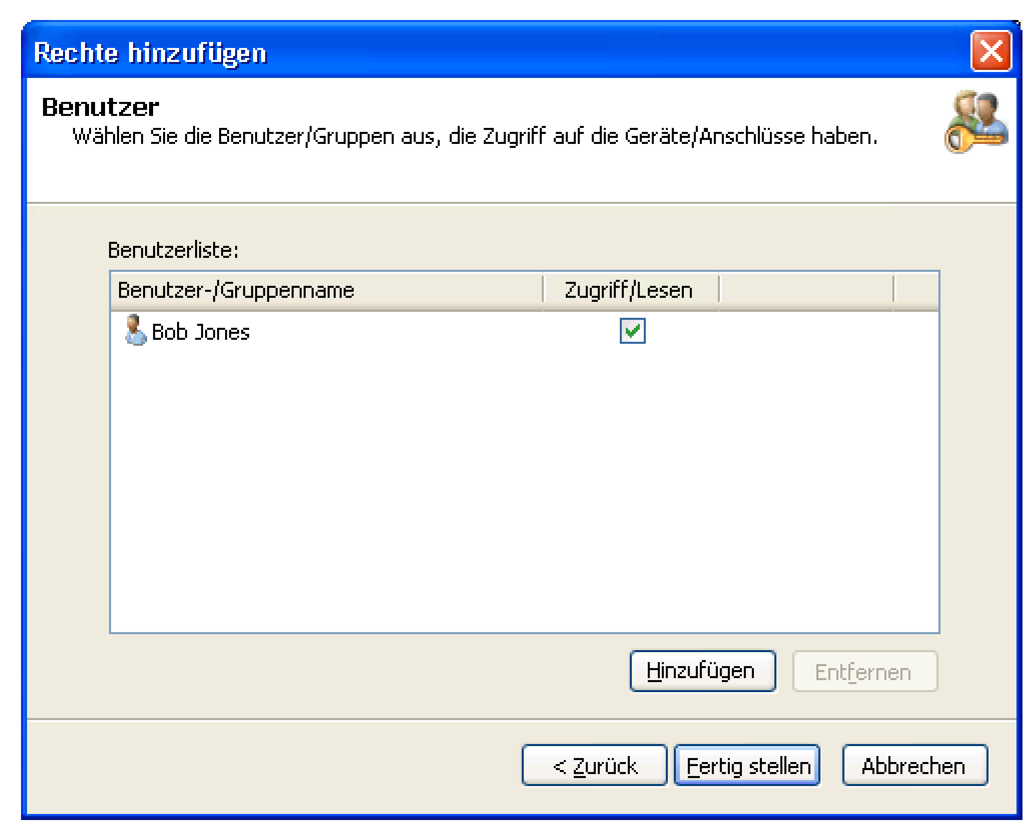

*Screenshot 67 - Optionen zum Hinzufügen von Berechtigungen - Schnittstellen*

7. Aktivieren oder deaktivieren Sie die gewünschten Schnittstellen, für die Berechtigungen konfiguriert werden sollen. Klicken Sie anschließend auf **Weiter**.




*Screenshot 68 - Optionen zum Hinzufügen von Berechtigungen - Benutzer*

8. Klicken Sie auf **Hinzufügen...**, um die Benutzer/Gruppen festzulegen, die auf die festgelegten Schnittstellen in dieser Schutzrichtlinie Zugriff haben. Klicken Sie anschließend auf **OK**.




*Screenshot 69 - Optionen zum Hinzufügen von Berechtigungen - Benutzer*

9. Aktivieren oder deaktivieren Sie die Berechtigungen **Zugriff/Lesen** für festgelegte Benutzer/Gruppen. Klicken Sie anschließend auf **Fertig stellen**.

So stellen Sie Aktualisierungen für Schutzrichtlinien auf den von der Schutzrichtlinie kontrollierten Computern bereit:

1. Klicken Sie in der GFI EndPointSecurity-Verwaltungskonsole auf die Registerkarte **Konfiguration**.

2. Klicken Sie auf die untergeordnete Registerkarte **Computer**.

3. Klicken Sie im linken Bereich im Abschnitt **Allgemeine Aufgaben** auf den Hyperlink **Auf allen Computern bereitstellen...**.

## 9.7 Konfigurieren von Zugriffsberechtigungen für einzelne Geräte

GFI EndPointSecurity bietet Ihnen die Möglichkeit, Berechtigungen für Schnittstellen den Active Directory (AD)-Benutzern und/oder -Benutzergruppen, oder lokalen Benutzern und/oder Benutzerschemen zuzuweisen. Diese Konfiguration kann für jede einzelne Richtlinie erfolgen.

Beispielsweise können Sie für einen bestimmten unternehmensintern erlaubten USB-Speicherstick den Lesezugriff erlauben. Versuche, auf andere USB-Sticks zuzugreifen, werden hingegen blockiert.



Führen Sie für eine Liste von Geräten, die momentan an kontrollierten Computern angeschlossen sind, einen Geräte-Scan durch, und fügen Sie die erkannten Geräte der Gerätedatenbank hinzu, um Zugriffsberechtigungen für einzelne Geräte zu konfigurieren. Weitere Informationen zum Geräte-Scan finden Sie im Kapitel Erkennen von Geräten in diesem Handbuch.

So konfigurieren Sie Benutzerberechtigungen für den Zugriff auf einzelne Geräte innerhalb einer Schutzrichtlinie:

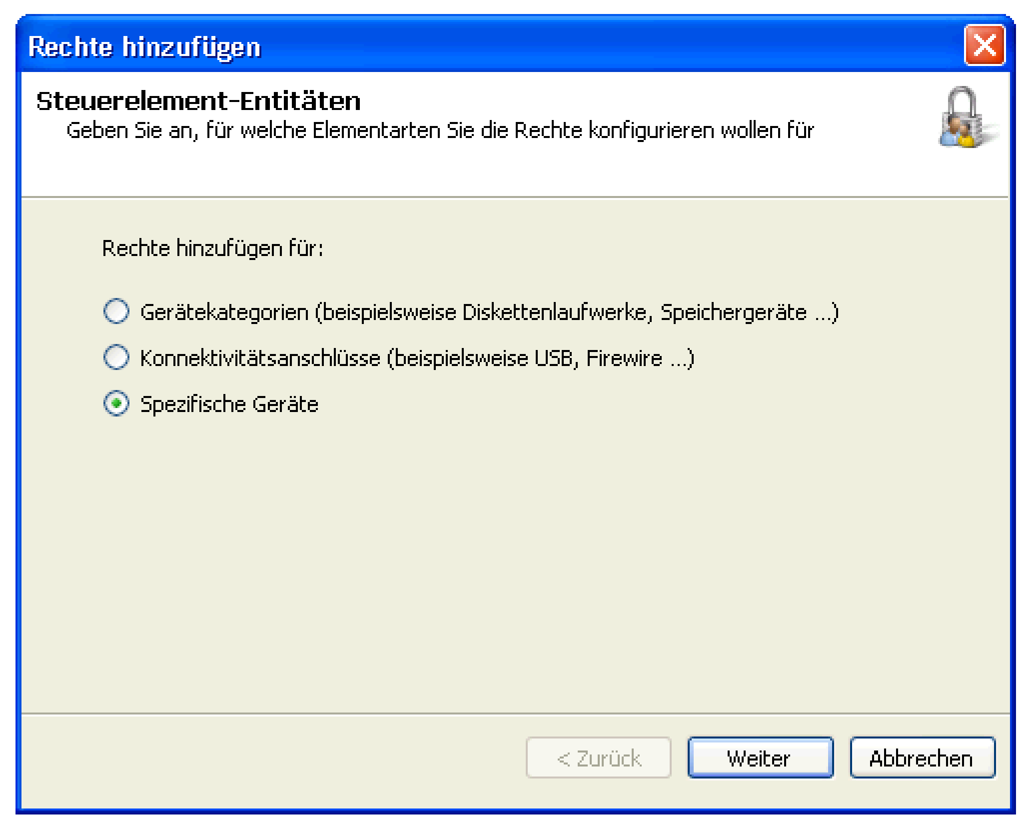
1. Klicken Sie in der GFI EndPointSecurity-Verwaltungskonsole auf die Registerkarte **Konfiguration**.

2. Klicken Sie auf die untergeordnete Registerkarte **Schutzrichtlinien.**

3. Wählen Sie im linken Bereich die zu konfigurierende Schutzrichtlinie aus.

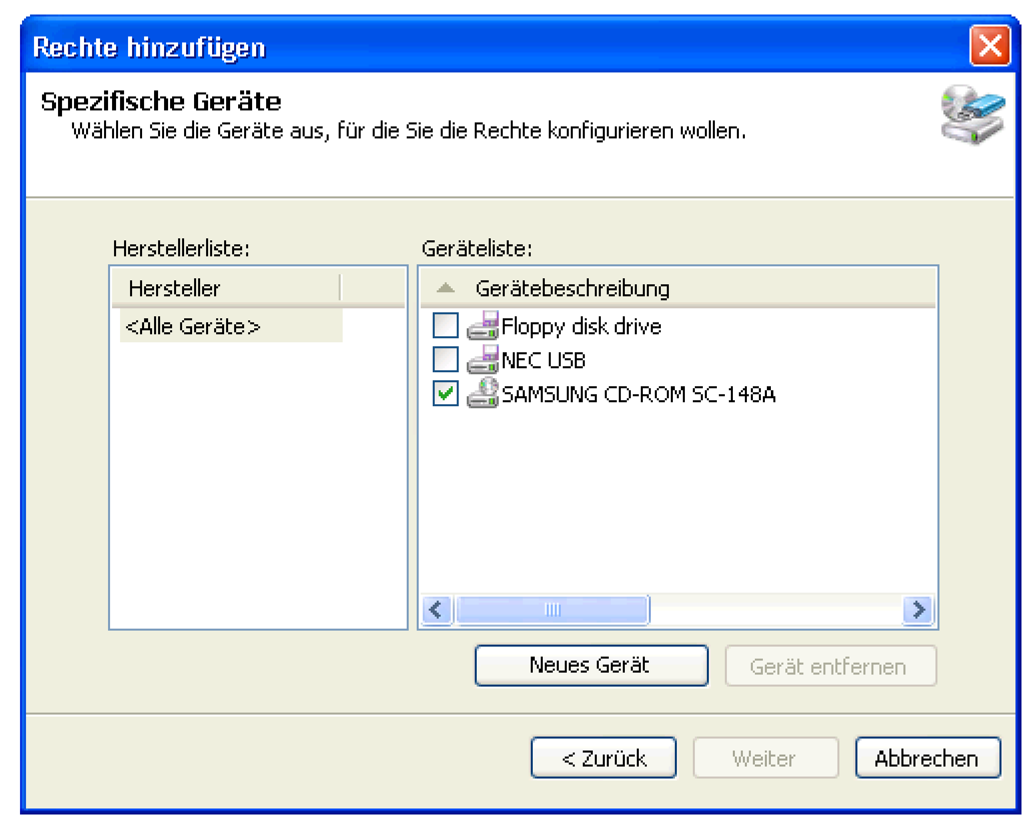
4. Klicken Sie auf den Unterknoten **Sicherheit**.

5. Klicken Sie im linken Bereich im Abschnitt **Allgemeine Aufgaben** auf den Hyperlink **Berechtigung(en) hinzufügen....**




*Screenshot 70 - Optionen zum Hinzufügen von Berechtigungen - Steuerung*

6. Wählen Sie im Dialog **Berechtigungen hinzufügen** die Option **Einzelne Geräte**, und klicken Sie zum Fortfahren auf **Weiter**.

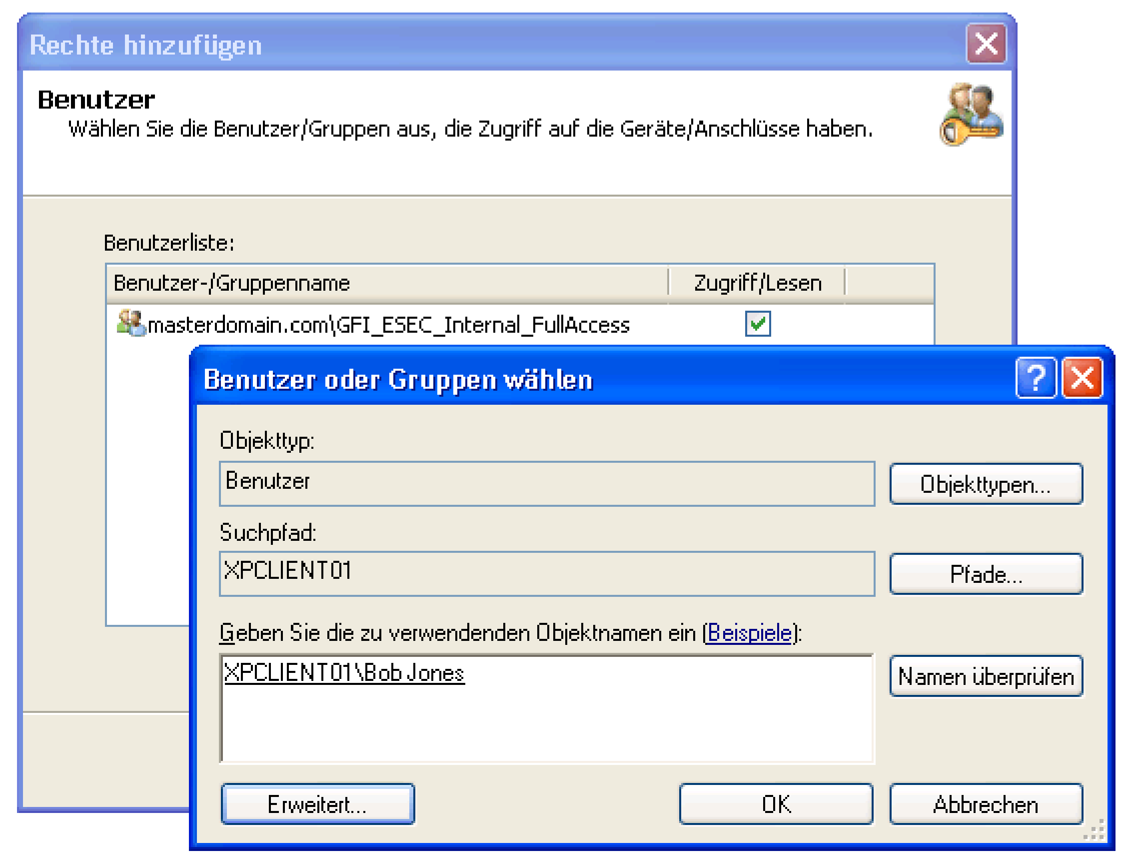



*Screenshot 71 - Optionen zum Hinzufügen von Berechtigungen - Einzelne Geräte*

7. Aktivieren oder deaktivieren Sie die gewünschten Geräte in der **Geräteliste**, für die Berechtigungen konfiguriert werden sollen. Klicken Sie anschließend auf **Weiter**.

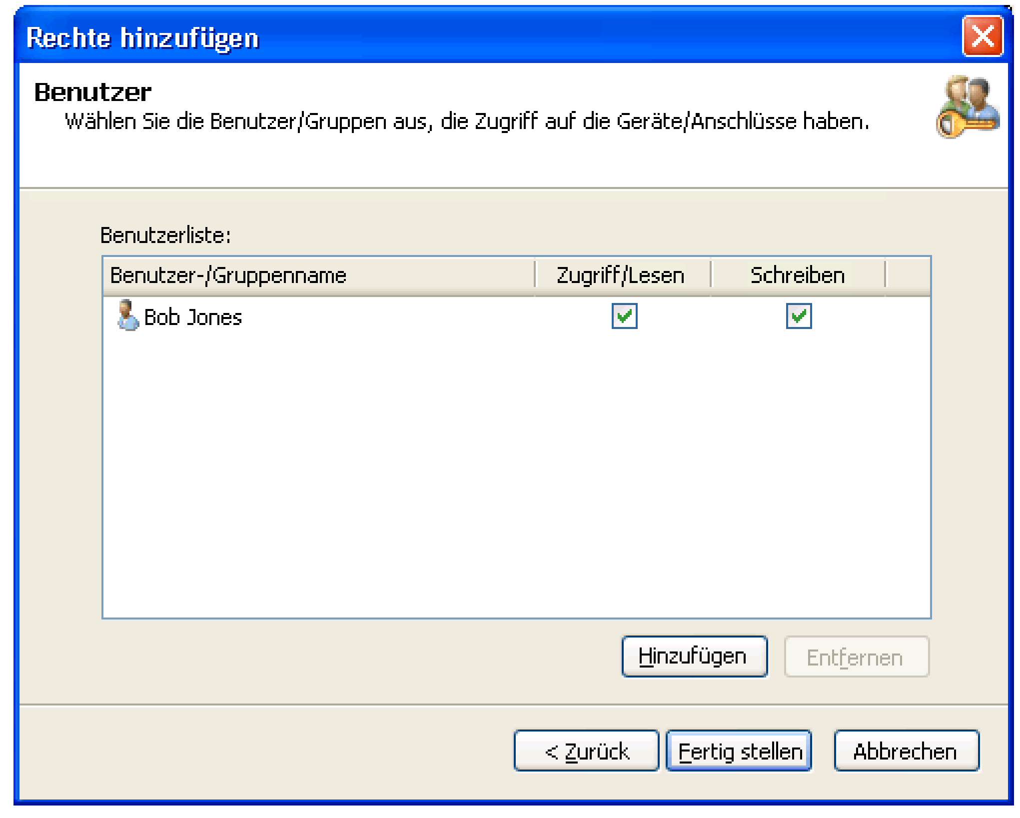


Falls ein gewünschtes Gerät nicht aufgelistet ist, klicken Sie auf **Neues Gerät**, um die Details des Geräts, für das Berechtigungen konfiguriert werden sollen, festzulegen. Klicken Sie anschließend auf **OK**.




*Screenshot 72 - Optionen zum Hinzufügen von Berechtigungen - Benutzer*

8. Klicken Sie auf **Hinzufügen...**, um die Benutzer/Gruppen festzulegen, die auf die festgelegten Geräte in dieser Schutzrichtlinie Zugriff haben. Klicken Sie anschließend auf **OK**.




*Screenshot 73 - Optionen zum Hinzufügen von Berechtigungen - Benutzer*

9. Aktivieren oder deaktivieren Sie die Berechtigungen **Zugriff/Lesen** und **Schreiben** für festgelegte Benutzer/Gruppen. Klicken Sie anschließend auf **Fertig stellen**.

So stellen Sie Aktualisierungen für Schutzrichtlinien auf den von der Schutzrichtlinie kontrollierten Computern bereit:

1. Klicken Sie in der GFI EndPointSecurity-Verwaltungskonsole auf die Registerkarte **Konfiguration**.

2. Klicken Sie auf die untergeordnete Registerkarte **Computer**.

3. Klicken Sie im linken Bereich im Abschnitt **Allgemeine Aufgaben** auf den Hyperlink **Auf allen Computern bereitstellen...**.

## 9.8 Anzeigen von Zugriffsberechtigungen

GFI EndPointSecurity bietet Ihnen die Möglichkeit, alle Berechtigungen anzuzeigen, die Active Directory (AD)-Benutzern und/oder -Benutzergruppen, oder lokalen Benutzern und/oder Benutzerschemen zugewiesen sind. Diese Konfiguration kann für jede einzelne Richtlinie erfolgen.



Wenn eine Gerätekategorie oder Schnittstelle nicht durch eine Schutzrichtlinie kontrolliert wird, ist die jeweilige Berechtigung deaktiviert. Weitere Informationen zum Hinzufügen oder Entfernen der Schutzrichtlinie von Gerätekategorien oder Schnittstellen finden Sie im Abschnitt Konfigurieren kontrollierter Gerätekategorien oder Konfigurieren kontrollierter Schnittstellen in diesem Kapitel.

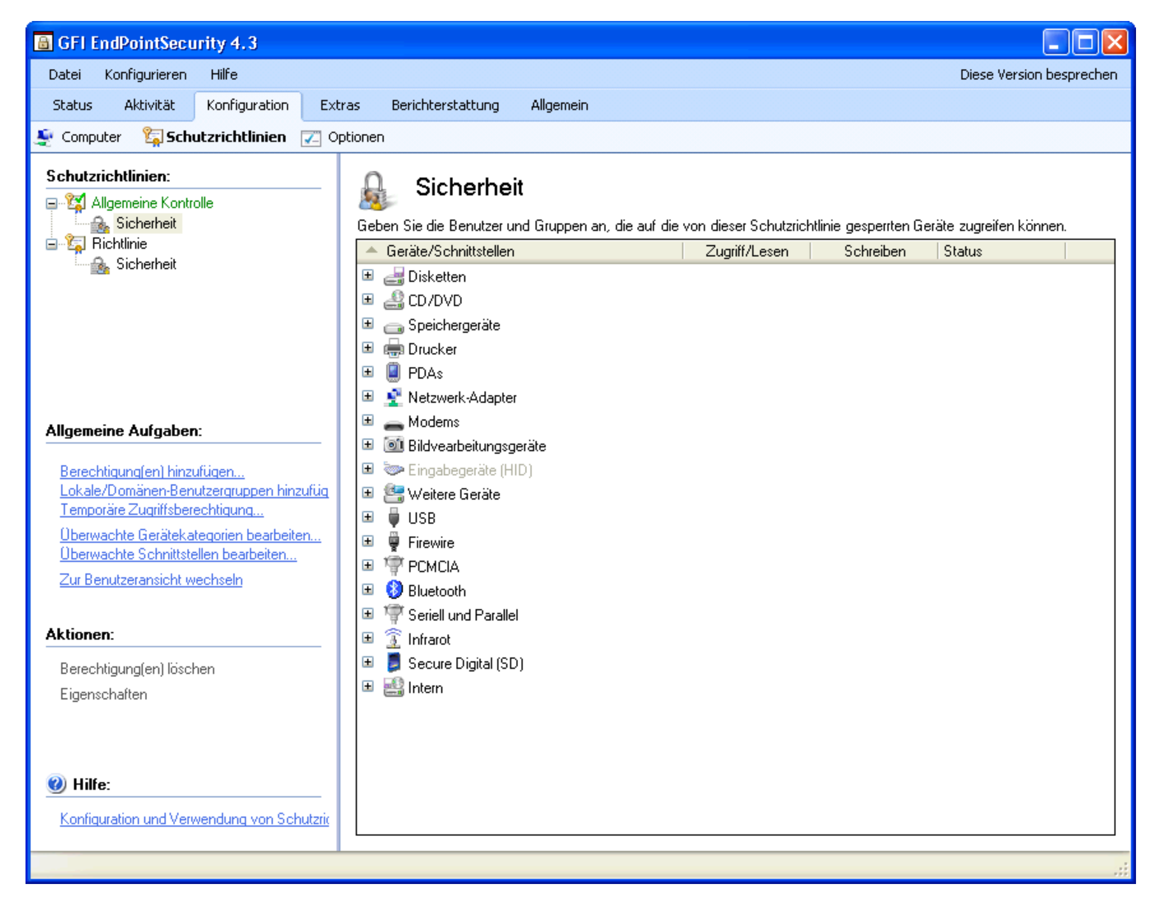
So zeigen Sie alle Benutzerberechtigungen für eine Schutzrichtlinie fest:

1. Klicken Sie in der GFI EndPointSecurity-Verwaltungskonsole auf die Registerkarte **Konfiguration**.

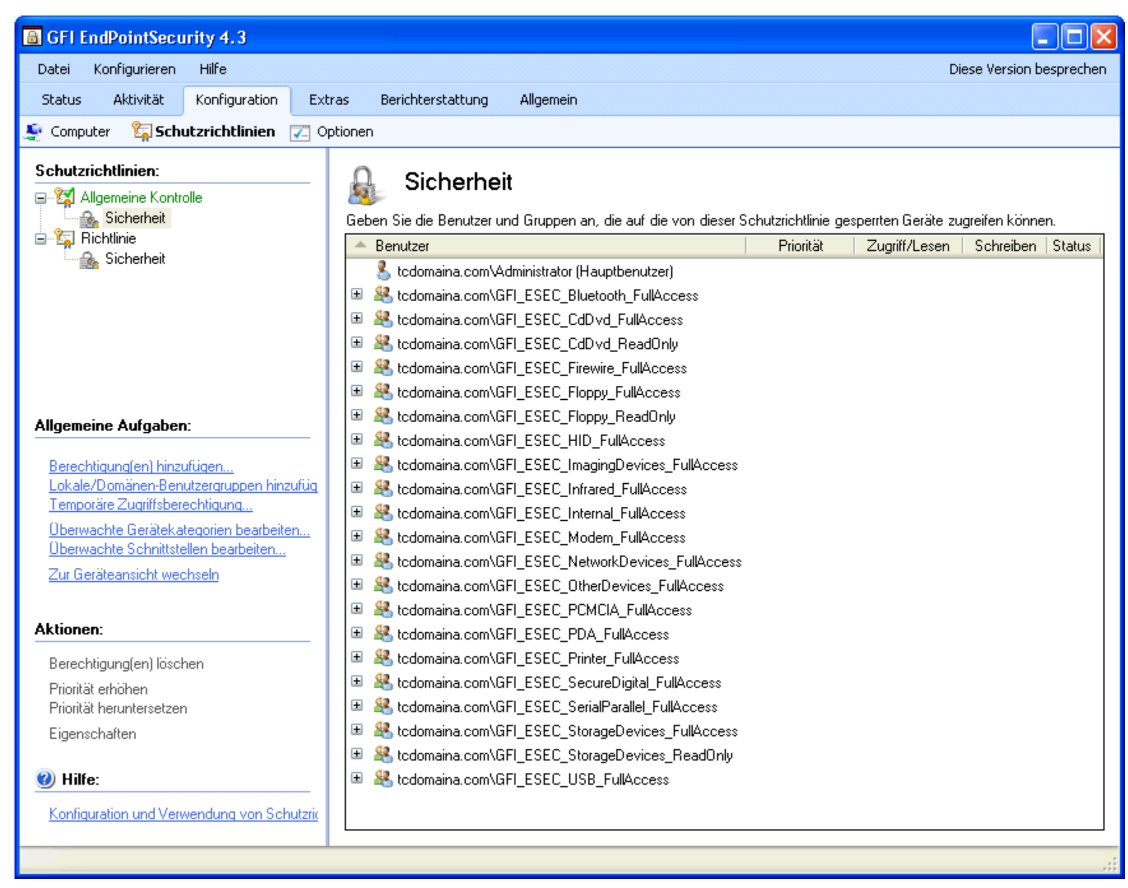
2. Klicken Sie auf die untergeordnete Registerkarte **Schutzrichtlinien**.

3. Wählen Sie im linken Bereich die Schutzrichtlinie aus, deren Berechtigungen Sie anzeigen möchten.

4. Klicken Sie auf den Unterknoten **Sicherheit**. Im rechten Bereich werden alle für die Schutzrichtlinie festgelegten Berechtigungen angezeigt.




*Screenshot 74 - Untergeordnete Registerkarte „Schutzrichtlinien“ - Geräteanzeige*




*Screenshot 75 - Untergeordnete Registerkarte „Schutzrichtlinien“ - Benutzeranzeige*

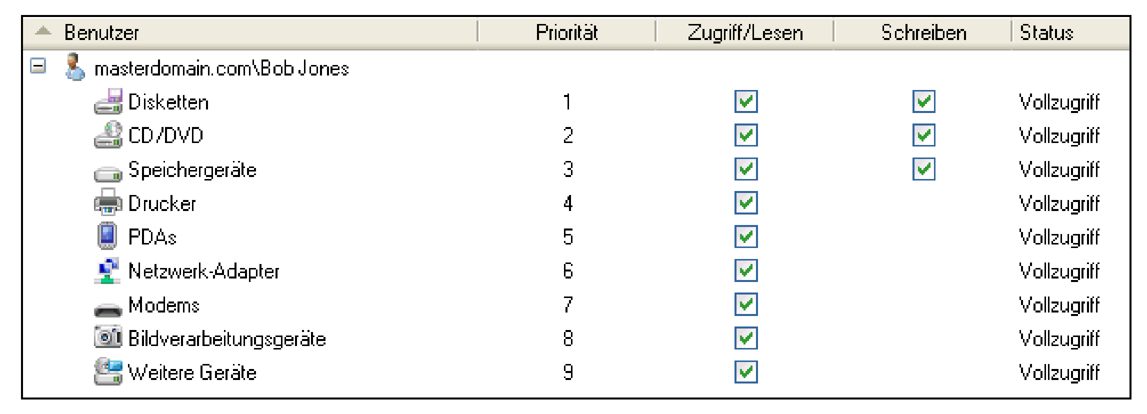
5. Klicken Sie im linken Bereich im Abschnitt **Allgemeine Aufgaben** auf den Hyperlink **Zur Geräteansicht wechseln** oder auf den Hyperlink **Zur Benutzeransicht wechseln**, um Berechtigungen gruppiert nach Gerät/Schnittstelle oder Benutzer anzuzeigen.

In der Benutzeransicht sehen Sie zudem die für die Schutzrichtlinie festgelegten Hauptbenutzer.

## 9.9 Konfigurieren von Berechtigungsprioritäten

GFI EndPointSecurity bietet Ihnen die Möglichkeit, Berechtigungen zu priorisieren, die Active Directory (AD)-Benutzern und/oder -Benutzergruppen, oder lokalen Benutzern und/oder Benutzerschemen zugewiesen sind. Diese Konfiguration kann für jede einzelne Richtlinie und jeden Benutzer erfolgen.

Beispielsweise können Sie benutzerspezifisch innerhalb einer Schutzrichtlinie angeben, dass die Zugriffsberechtigungen für USB-Schnittstellen die Priorität 1 haben sollen, während für CD-/DVD-Laufwerke die Priorität 2 gilt. Schließt in diesem Fall ein Benutzer ein externes CD-/DVD-Laufwerk über die USB-Schnittstelle an einen kontrollierten Computer an, haben die USB-Zugriffsberechtigungen Vorrang vor denen des CD-/DVD-Laufwerks.



| Benutzer | Priorität | Zugriff/Lesen | Schreiben | Status |
|---|---|---|---|---|
| masterdomain.com\Bob Jones | | | | |
| Disketten | 1 | ✓ | ✓ | Vollzugriff |
| CD/DVD | 2 | ✓ | ✓ | Vollzugriff |
| Speichergeräte | 3 | ✓ | ✓ | Vollzugriff |
| Drucker | 4 | ✓ | | Vollzugriff |
| PDAs | 5 | ✓ | | Vollzugriff |
| Netzwerk-Adapter | 6 | ✓ | | Vollzugriff |
| Modems | 7 | ✓ | | Vollzugriff |
| Bildverarbeitungsgeräte | 8 | ✓ | | Vollzugriff |
| Weitere Geräte | 9 | ✓ | | Vollzugriff |

*Screenshot 76 - Untergeordnete Registerkarte „Schutzrichtlinien“ - Bereich „Sicherheit“*

So priorisieren Sie Benutzerberechtigungen für eine Schutzrichtlinie:

1. Klicken Sie in der GFI EndPointSecurity-Verwaltungskonsole auf die Registerkarte **Konfiguration**.

2. Klicken Sie auf die untergeordnete Registerkarte **Schutzrichtlinien**.

3. Wählen Sie im linken Bereich die Schutzrichtlinie aus, für deren Berechtigungen Sie Prioritäten festlegen möchten.

4. Klicken Sie auf den Unterknoten **Sicherheit**.

5. Klicken Sie im linken Bereich im Abschnitt **Allgemeine Aufgaben** auf den Hyperlink **Zur Benutzeransicht wechseln**, um nach Benutzern gruppierte Berechtigungen anzuzeigen.

6. Klicken Sie mit der rechten Maustaste in den Abschnitt **Sicherheit**, und wählen Sie **Alle erweitern** aus.

7. Markieren Sie das gewünschte Gerät oder die gewünschte Schnittstelle.

8. Klicken Sie im linken Bereich im Abschnitt **Aktionen** auf den Hyperlink **Priorität erhöhen** oder auf den Hyperlink **Priorität heruntersetzen**.

So stellen Sie Aktualisierungen für Schutzrichtlinien auf den von der Schutzrichtlinie kontrollierten Computern bereit:

1. Klicken Sie in der GFI EndPointSecurity-Verwaltungskonsole auf die Registerkarte **Konfiguration**.

2. Klicken Sie auf die untergeordnete Registerkarte **Computer**.

3. Klicken Sie im linken Bereich im Abschnitt **Allgemeine Aufgaben** auf den Hyperlink **Auf allen Computern bereitstellen....**

## 9.10 Konfigurieren der Geräte-Blacklist

GFI EndPointSecurity bietet Ihnen die Möglichkeit, Geräte festzulegen, auf die nicht jeder Zugriff hat. Mithilfe einer differenzierten Blacklist können sogar per Seriennummer identifizierte Einzelgeräte blockiert werden. Diese Konfigurierung kann für jede einzelne Richtlinie erfolgen.



Führen Sie für eine Liste von Geräten, die momentan an kontrollierten Computern angeschlossen sind, einen Geräte-Scan durch, und fügen Sie die erkannten Geräte der Gerätedatenbank hinzu, bevor Sie sie der Geräte-Blacklist hinzufügen. Weitere Informationen zum Geräte-Scan finden Sie im Kapitel Erkennen von Geräten in diesem Handbuch.



Hauptbenutzer können auf alle Geräte auf der Blacklist zugreifen.

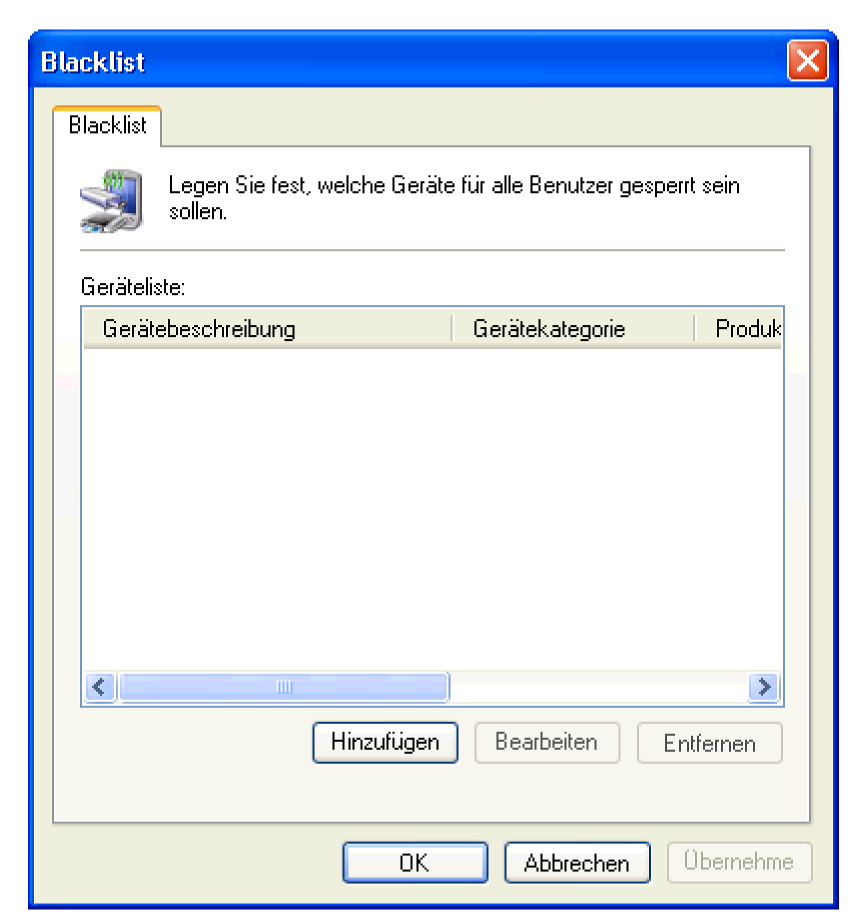
So fügen Sie Geräte einer Schutzrichtlinie der Blacklist hinzu:

1. Klicken Sie in der GFI EndPointSecurity-Verwaltungskonsole auf die Registerkarte **Konfiguration**.

2. Klicken Sie auf die untergeordnete Registerkarte **Schutzrichtlinien**.

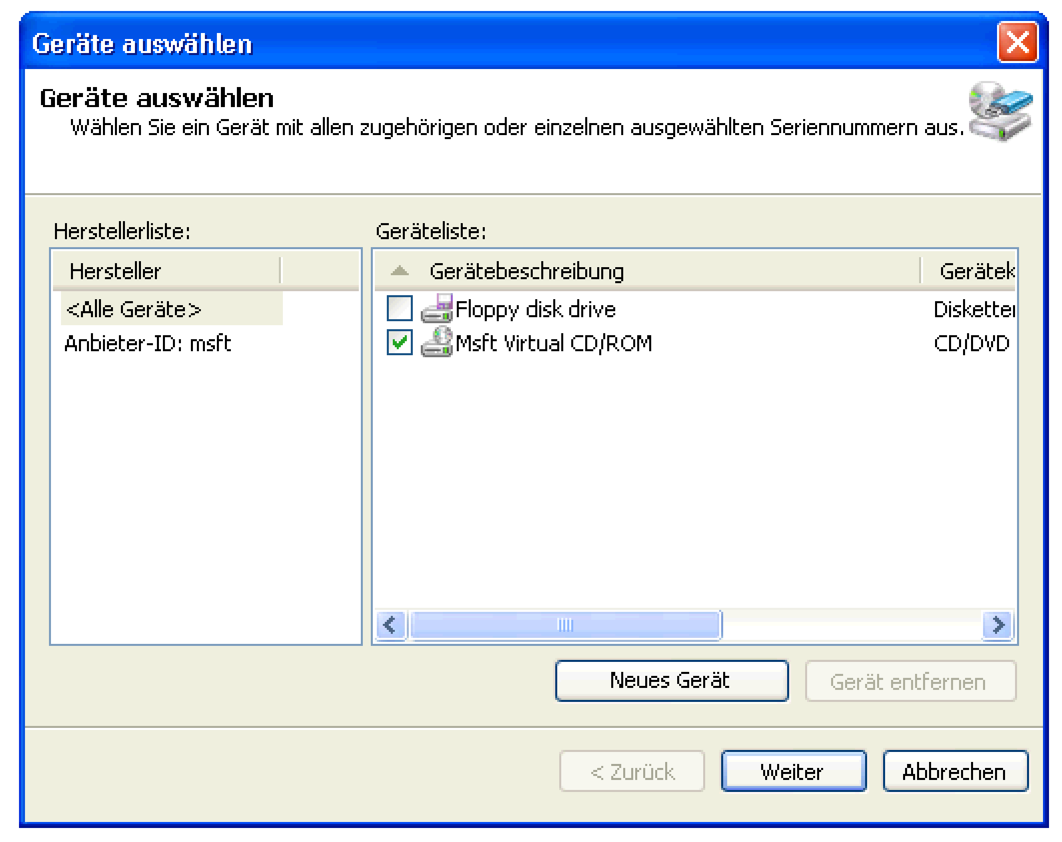
3. Wählen Sie im linken Bereich die Schutzrichtlinie aus, für die Geräte auf die Blacklist gesetzt werden sollen.

4. Klicken Sie im rechten Bereich im Abschnitt **Sicherheit** auf den Hyperlink **Geräte-Blacklist**.




*Screenshot 77 - Blacklist-Optionen*

5. Klicken Sie im Dialog **Blacklist** auf die Option **Hinzufügen…**, um Geräte für die Blacklist auszuwählen.

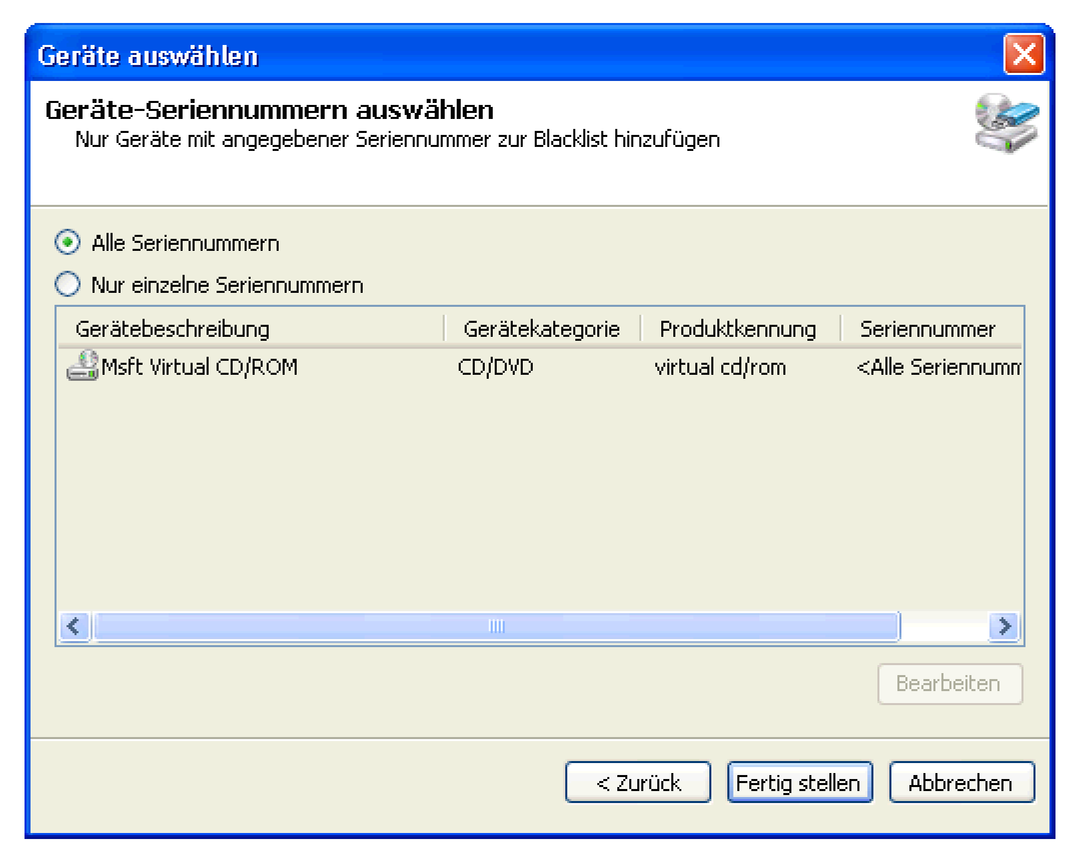



*Screenshot 78 - Optionen zur Geräteauswahl*

6. Aktivieren oder deaktivieren Sie im Dialog **Geräte auswählen** die Geräte, die aus der **Geräteliste** der Blacklist hinzugefügt werden sollen. Klicken Sie anschließend auf **Weiter**.



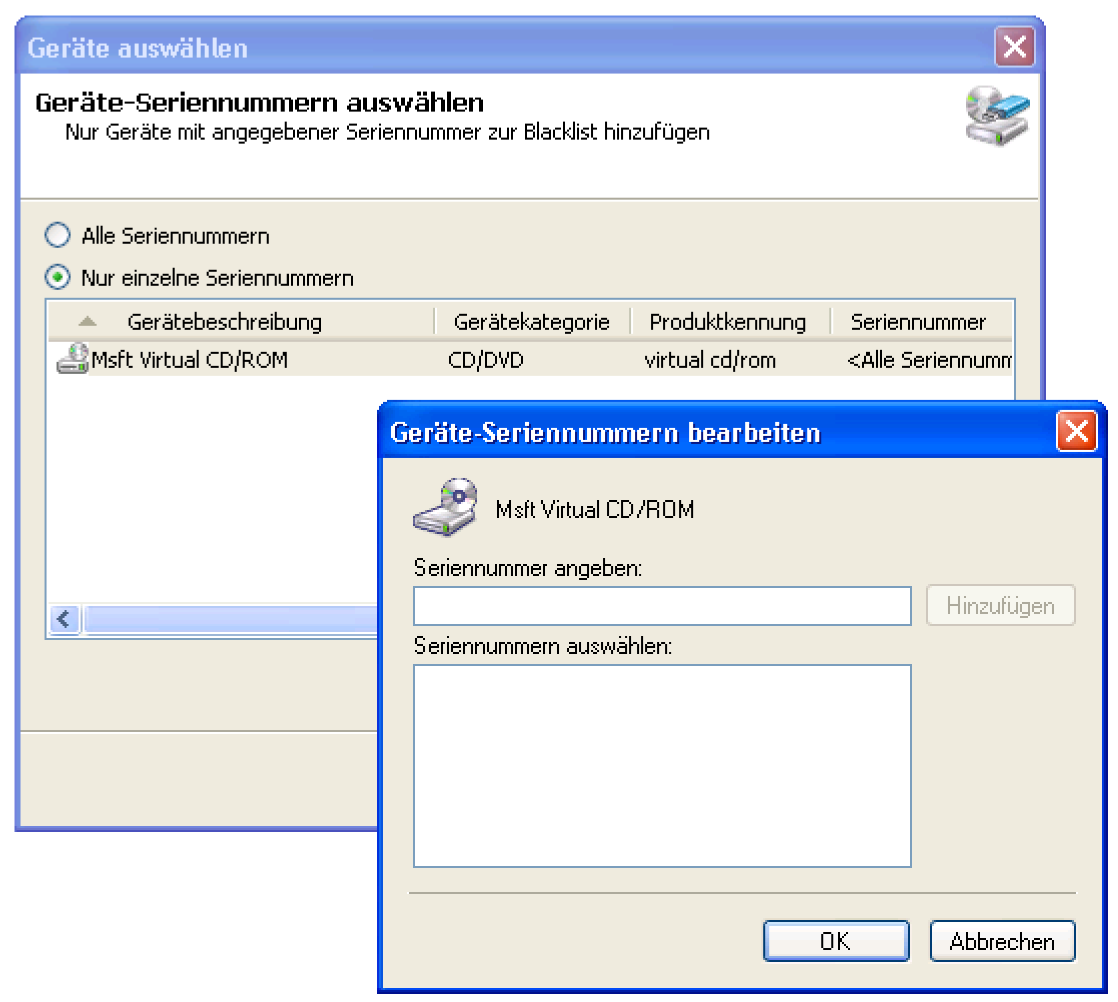
Falls ein gewünschtes Gerät nicht aufgelistet ist, klicken Sie auf **Neues Gerät hinzufügen…**, um die Details des Geräts, das der Blacklist hinzugefügt werden soll, festzulegen. Klicken Sie anschließend auf **OK**.




*Screenshot 79 - Optionen zur Geräteauswahl - Auswahl der Geräteseriennummer*

7. Wählen Sie die gewünschte Option für die Seriennummern aus:

» **Alle Seriennummer** - Um alle Seriennummern eines Geräts der Blacklist hinzuzufügen. Klicken Sie auf **Fertig stellen** und **OK**.




*Screenshot 80 - Optionen zur Geräteauswahl - Bearbeiten der Geräteseriennummern*

» **Nur einzelne Seriennummern** - Um nur die Seriennummern bestimmter Geräte der Blacklist hinzuzufügen. Markieren Sie anschließend das Gerät, und klicken Sie auf **Bearbeiten…**, um eine Seriennummer der Blacklist hinzuzufügen. Klicken Sie auf **OK**, **Fertig stellen** und **OK**.

So stellen Sie Aktualisierungen für Schutzrichtlinien auf den von der Schutzrichtlinie kontrollierten Computern bereit:

1. Klicken Sie in der GFI EndPointSecurity-Verwaltungskonsole auf die Registerkarte **Konfiguration**.

2. Klicken Sie auf die untergeordnete Registerkarte **Computer**.

3. Klicken Sie im linken Bereich im Abschnitt **Allgemeine Aufgaben** auf den Hyperlink **Auf allen Computern bereitstellen....**

## 9.11 Konfigurieren der Geräte-Whitelist

GFI EndPointSecurity bietet Ihnen die Möglichkeit, Geräte festzulegen, auf die jeder Zugriff hat. Mithilfe einer differenzierten Whitelist können sogar bestimmte, per Seriennummer identifizierte Einzelgeräte zugänglich gemacht werden. Diese Konfigurierung kann für jede einzelne Richtlinie erfolgen.



Führen Sie für eine Liste von Geräten, die momentan an kontrollierten Computern angeschlossen sind, einen Geräte-Scan durch, und fügen Sie die erkannten Geräte der Gerätedatenbank hinzu, bevor Sie sie der Geräte-Whitelist hinzufügen. Weitere Informationen zum Geräte-Scan finden Sie im Kapitel Erkennen von Geräten in diesem Handbuch.

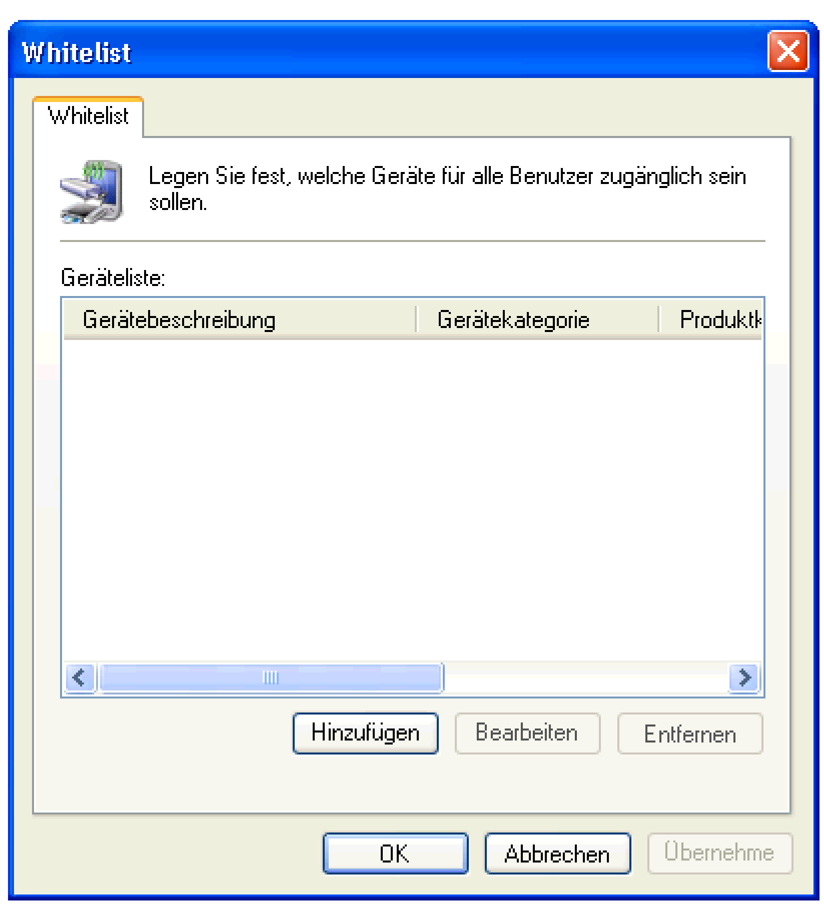
So fügen Sie Geräte einer Schutzrichtlinie der Whitelist hinzu:

1. Klicken Sie in der GFI EndPointSecurity-Verwaltungskonsole auf die Registerkarte **Konfiguration**.

2. Klicken Sie auf die untergeordnete Registerkarte **Schutzrichtlinien**.

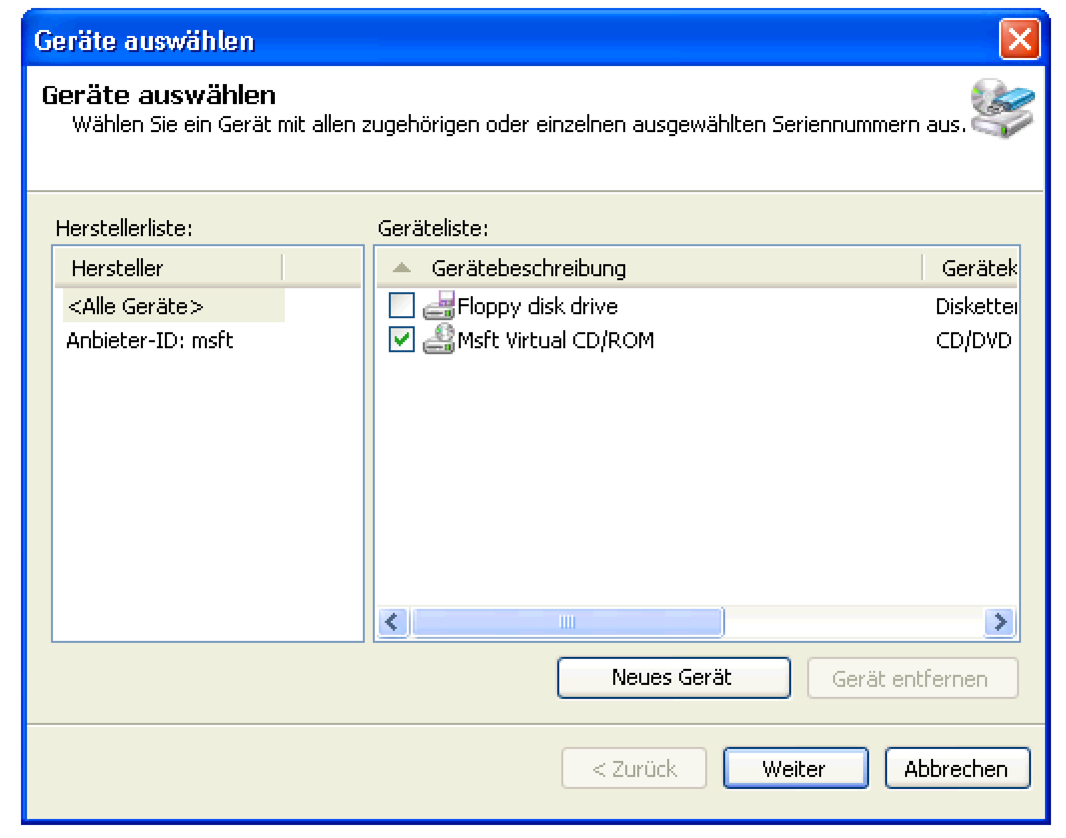
3. Wählen Sie im linken Bereich die Schutzrichtlinie aus, für die Geräte auf die Whitelist gesetzt werden sollen.

4. Klicken Sie im rechten Bereich im Abschnitt **Sicherheit** auf den Hyperlink **Geräte-Whitelist**.




*Screenshot 81 - Whitelist-Optionen*

5. Klicken Sie im Dialog **Whitelist** auf die Option **Hinzufügen…**, um Geräte für die Whitelist auszuwählen.

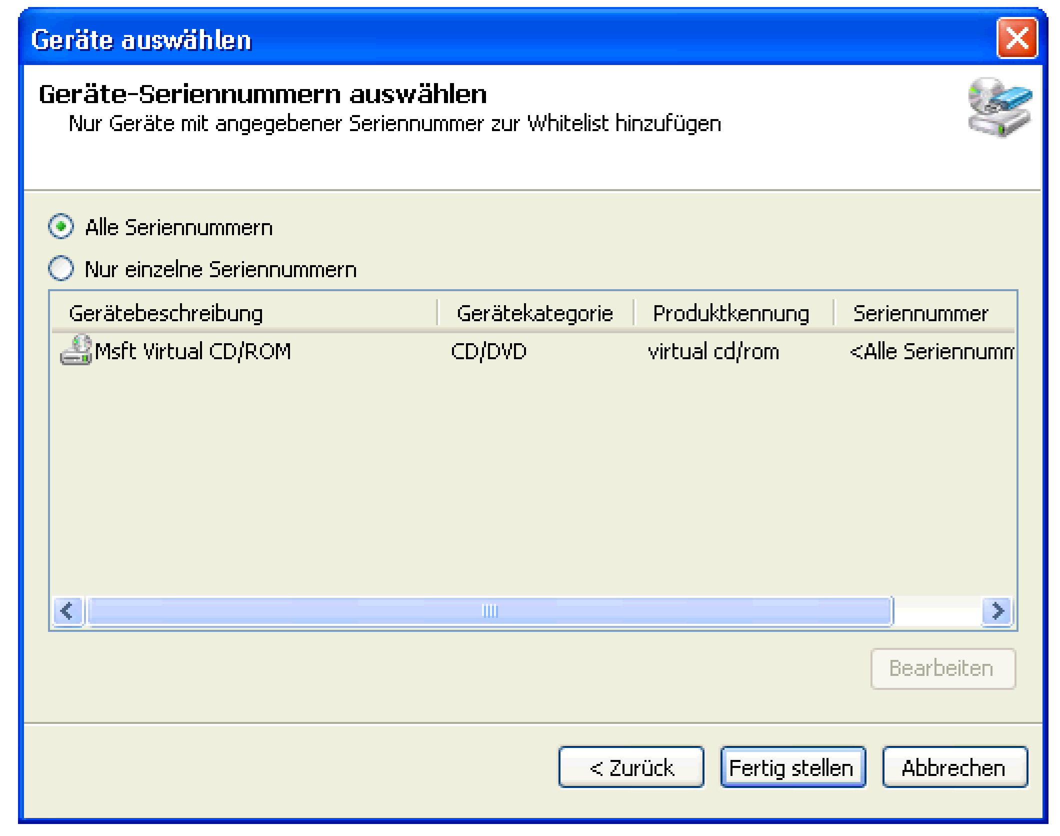



*Screenshot 82 - Optionen zur Geräteauswahl*

6. Aktivieren oder deaktivieren Sie im Dialog **Geräte auswählen** die Geräte, die aus der **Geräteliste** der Whitelist hinzugefügt werden sollen. Klicken Sie anschließend auf **Weiter**.



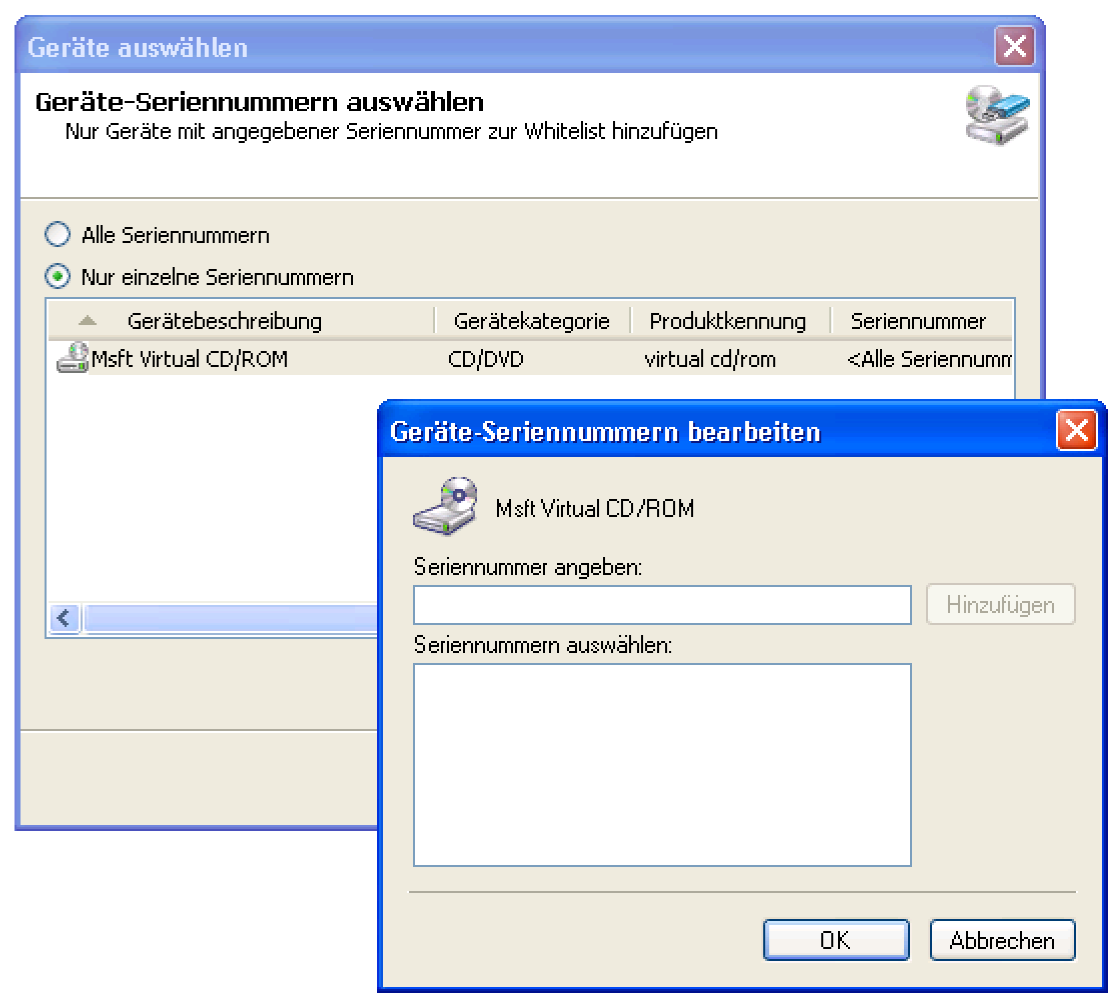
Falls ein gewünschtes Gerät nicht aufgelistet ist, klicken Sie auf **Neues Gerät hinzufügen…**, um die Details des Geräts, das der Whitelist hinzugefügt werden soll, festzulegen. Klicken Sie anschließend auf **OK**.




*Screenshot 83 - Optionen zur Geräteauswahl - Auswahl der Geräteseriennummer*

7. Wählen Sie die gewünschte Option für die Seriennummern aus:

- **Alle Seriennummer** - Um alle Seriennummern eines Geräts der Whitelist hinzuzufügen. Klicken Sie auf **Fertig stellen** und **OK**.




*Screenshot 84 - Optionen zur Geräteauswahl - Bearbeiten der Geräteseriennummern*

- **Nur einzelne Seriennummern** - Um nur die Seriennummern bestimmter Geräte der Whitelist hinzuzufügen. Markieren Sie anschließend das Gerät, und klicken Sie auf **Bearbeiten…**, um eine Seriennummer der Whitelist hinzuzufügen. Klicken Sie auf **OK**, **Fertig stellen** und **OK**.

So stellen Sie Aktualisierungen für Schutzrichtlinien auf den von der Schutzrichtlinie kontrollierten Computern bereit:

1. Klicken Sie in der GFI EndPointSecurity-Verwaltungskonsole auf die Registerkarte **Konfiguration**.

2. Klicken Sie auf die untergeordnete Registerkarte **Computer**.

3. Klicken Sie im linken Bereich im Abschnitt **Allgemeine Aufgaben** auf den Hyperlink **Auf allen Computern bereitstellen....**

## 9.12 Konfigurieren zeitlich begrenzter Zugriffsrechte

GFI EndPointSecurity bietet Ihnen die Möglichkeit, den Zugriff von Benutzern auf Geräte und Schnittstellen auf kontrollierten Computern für eine bestimmte Dauer und ein bestimmtes Zeitfenster (wenn der Zugriff normalerweise blockiert wird) zu ermöglichen. Diese Konfigurierung kann für jede einzelne Richtlinie erfolgen.



Wenn ein zeitlich begrenzter Zugriff gewährt wird, werden alle Berechtigungen und Einstellungen (z. B. Dateityp-Filter) dieser Schutzrichtlinie für diesen Computer temporär aufgehoben.

Weitere Informationen zu Anfragen für zeitlich begrenzten Zugriff und entsprechende Berechtigungen finden Sie im Kapitel Informationen zu GFI EndPointSecurity unter Funktionsweise von GFI EndPointSecurity – Zeitlich begrenzter Zugriff.

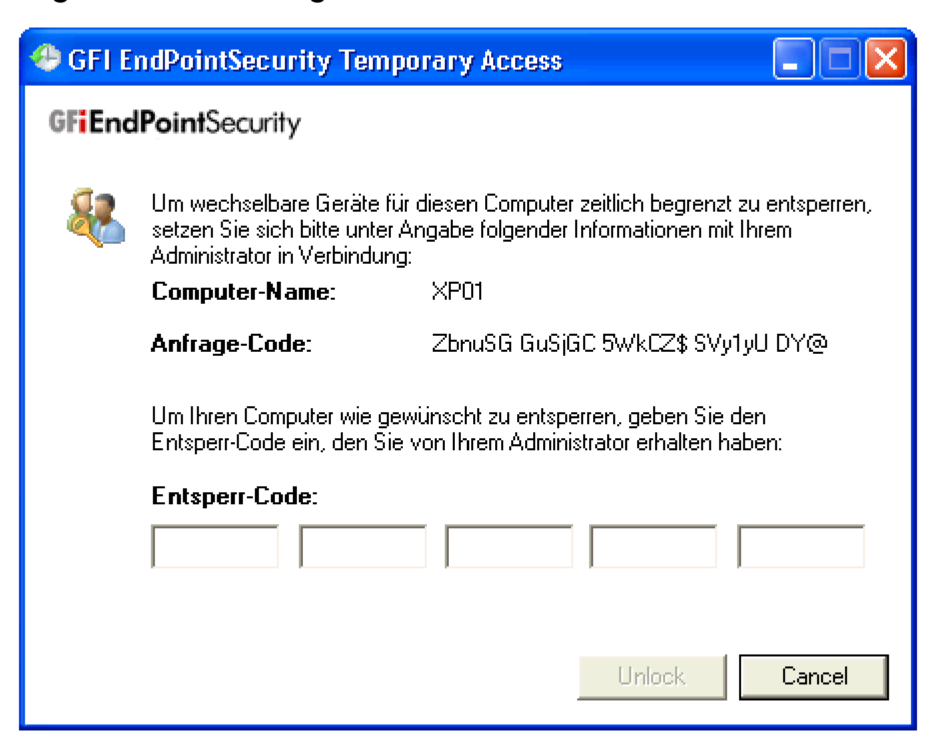
### 9.12.1 Beantragen des zeitlich begrenzten Zugriffs auf einen geschützten Computer

Um einen Anfragecode zu generieren, muss der Benutzer das **Temporary-Access-Tool von GFI EndPointSecurity** starten:




*Screenshot 85 - Symbol „Zeitlich begrenzter Gerätezugriff"*

1. Klicken Sie in der **Microsoft Windows-Systemsteuerung** auf das Symbol für den **zeitlich begrenzten Gerätezugriff**.




*Screenshot 86 - Temporary-Access-Tool von GFI EndPointSecurity*

2. Notieren Sie den **Abfragecode**, der im Dialog **GFI EndPointSecurity Temporary Access** angezeigt wird und teilen Sie diesen zusammen mit dem Gerätetyp und/oder der Schnittstelle, auf das/die zugegriffen werden soll, dem Systemadministrator mit. Dieser muss auch den Zeitraum für den Zugriff erfahren.

Das **Temporary-Access-Tool von GFI EndPointSecurity** kann geöffnet bleiben.

3. Nachdem Sie vom Administrator den Entsperrcode erhalten haben, geben Sie ihn in das Feld **Entsperrcode** ein.



Wird der Entsperrcode nicht innerhalb des festgelegten Zeitraums auf dem geschützten Computer eingegeben, ist kein Zugriff möglich.

4. Klicken Sie auf **Entsperren**, um den zeitlich begrenzten Zugriff zu aktivieren. Nun kann auf das gewünschte Geräte und/oder die Schnittstelle zugegriffen werden.

### 9.12.2 Gewähren des zeitlich begrenzten Zugriffs auf einen geschützten Computer

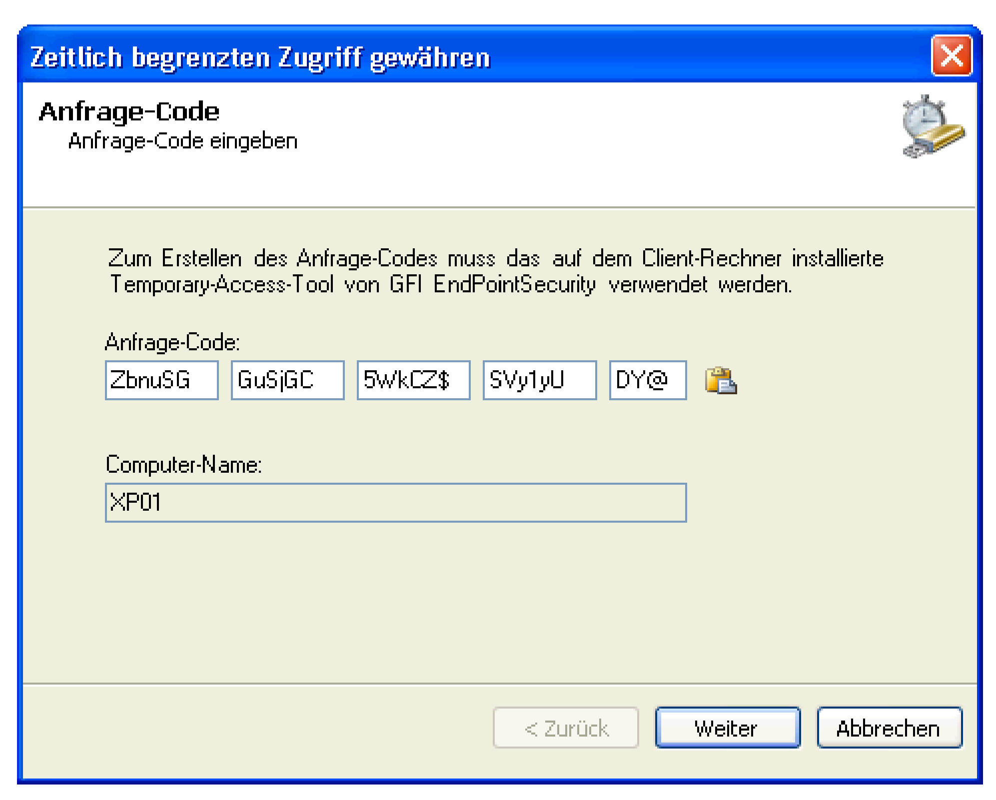
Um zeitlich begrenzten Zugriff zu gewähren, sollte der Administrator:

1. In der GFI EndPointSecurity-Verwaltungskonsole auf die Registerkarte **Konfiguration** klicken.

2. Auf die untergeordnete Registerkarte **Schutzrichtlinien** klicken.

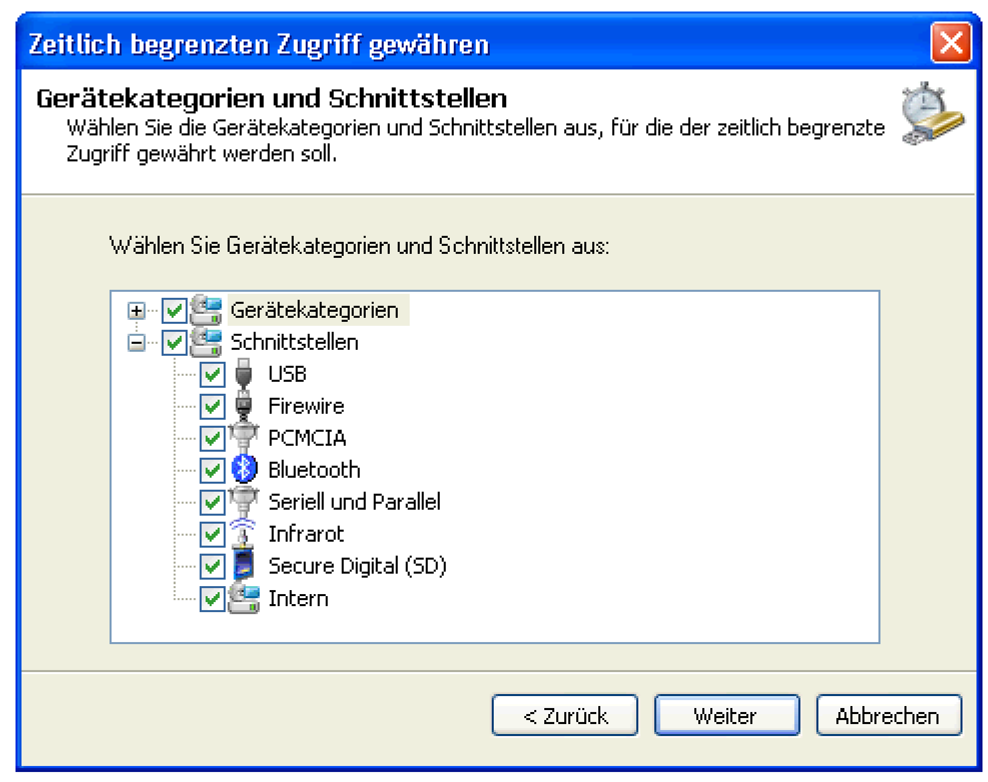
3. Im linken Bereich die Schutzrichtlinie auswählen, die den Computer kontrolliert, für den ein zeitlich begrenzter Zugriff gewährt werden soll.

4. Im rechten Bereich im Abschnitt **Zeitlich begrenzter Zugriff** auf den Hyperlink **Temporäre Zugriffsberechtigung** klicken.



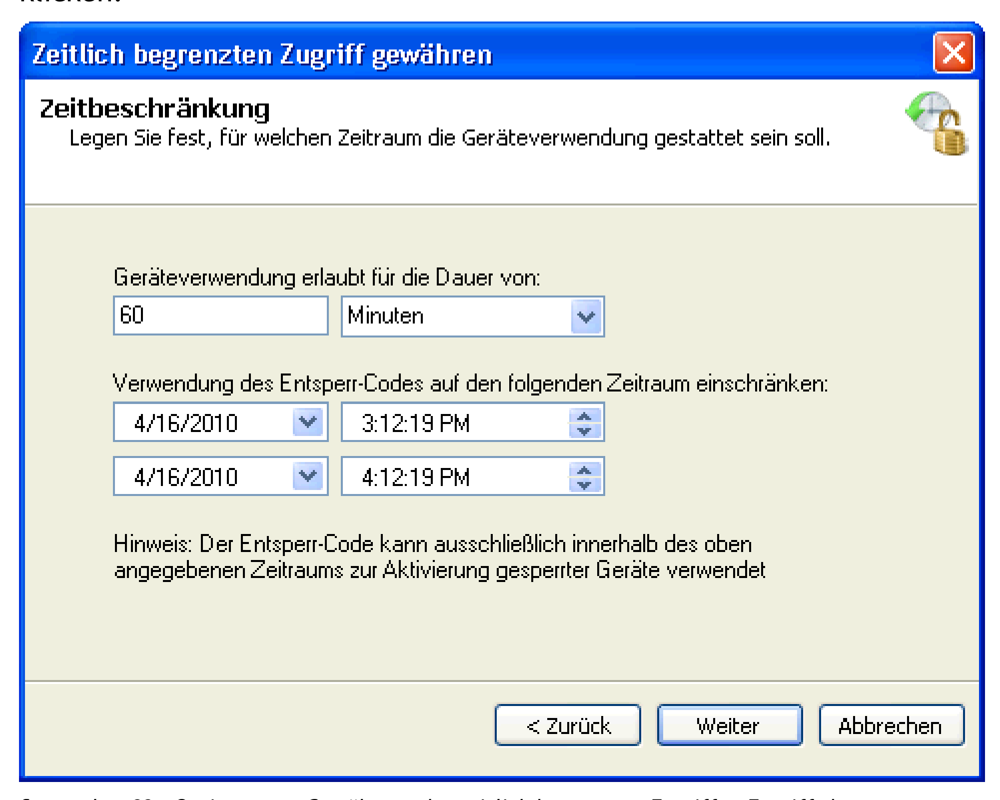

*Screenshot 87 - Optionen zur Gewährung des zeitlich begrenzten Zugriffs - Anfragecode*

5. Im Dialog **Temporäre Zugriffsberechtigung** den vom Benutzer erhaltenen Code in das Feld **Anfragecode** eingeben. Daraufhin wird der Name des Computers, von dem die Anfrage generiert wurde, im Feld **Computername** angezeigt. Anschließend muss der Administrator auf **Weiter** klicken.




*Screenshot 88 - Optionen zur Gewährung des zeitlich begrenzten Zugriffs - Gerätekategorien und Schnittstellen*

6. Die erforderlichen Gerätekategorien und/oder Schnittstellen in der Liste aktivieren, auf die Zugriff gewährt werden sollen. Anschließend muss der Administrator auf **Weiter** klicken.




*Screenshot 89 - Optionen zur Gewährung des zeitlich begrenzten Zugriffs - Zugriffsdauer*

7. Die Dauer des erlaubten Zugriffs und den Zeitraum angeben, in dem der Entsperrcode eingegeben werden muss. Anschließend muss der Administrator auf **Weiter** klicken.

8. Den erstellten **Entsperrcode** notieren und diesen dem Benutzer mitteilen, der den zeitlich begrenzten Zugriff angefragt hat. Anschließend muss der Administrator auf **Fertig stellen** klicken.

## 9.13 Konfigurieren der Dateitypfilter

GFI EndPointSecurity gibt Ihnen die Möglichkeit, Einschränkungen für Dateitypen zu definieren, beispielsweise für Dateien der Formate .doc oder .xls, um zu verhindern, dass diese auf oder von erlaubten Geräten kopiert werden. Diese Einschränkungen können Active Directory (AD)-Benutzern und/oder -Benutzergruppen, oder lokalen Benutzern und/oder Benutzerschemen zugewiesen werden. Diese Konfigurierung kann für jede einzelne Richtlinie erfolgen.

Die Filterung basiert auf der Überprüfung von Dateierweiterungen und Echtzeitüberprüfungen des wahren Dateityps. Die Echtzeitüberprüfung erfolgt für folgende Dateitypen:

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| AVI | BMP | CAB | CHM | DLL | DOC | EMF | EXE |
| GIF | HLP | HTM | JPE | JPEG | JPG | LNK | M4A |
| MDB | MP3 | MPEG | MPG | MSG | MSI | OCX | P7M |
| PDF | PPT | RAR | RTF | SCR | SYS | TIF | TIFF |
| TXT | URL | WAV | XLS | ZIP | | | |

Nicht aufgelistete Dateitypen werden nur basierend auf der Dateierweiterung gefiltert.



Die Dateityp-Filterung erfolgt nur für Gerätekategorien und/oder Schnittstellen, auf die zugegriffen werden kann.

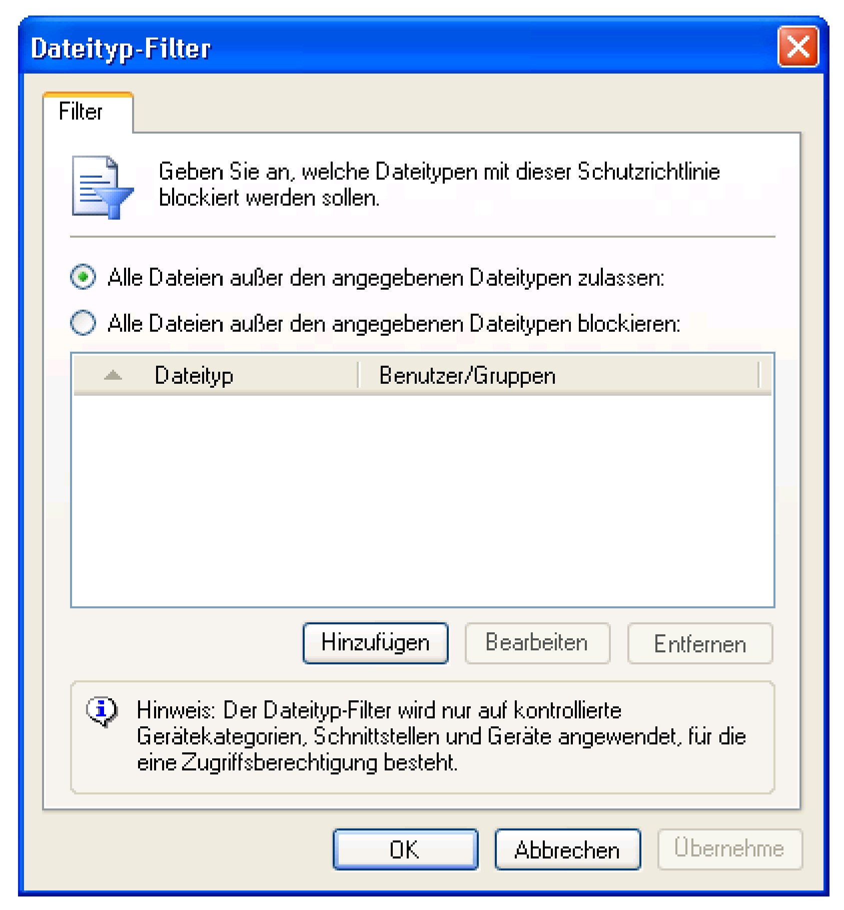
So konfigurieren Sie Dateitypeinschränkungen für Benutzer innerhalb einer Schutzrichtlinie:

1. Klicken Sie in der GFI EndPointSecurity-Verwaltungskonsole auf die Registerkarte **Konfiguration**.

2. Auf die untergeordnete Registerkarte **Schutzrichtlinien** klicken.

3. Wählen Sie im linken Bereich die Schutzrichtlinie aus, für die Sie Dateitypeinschränkungen definieren möchten.

4. Klicken Sie im rechten Bereich im Abschnitt **Dateiüberwachung** auf den Hyperlink **Dateityp-Filter**.

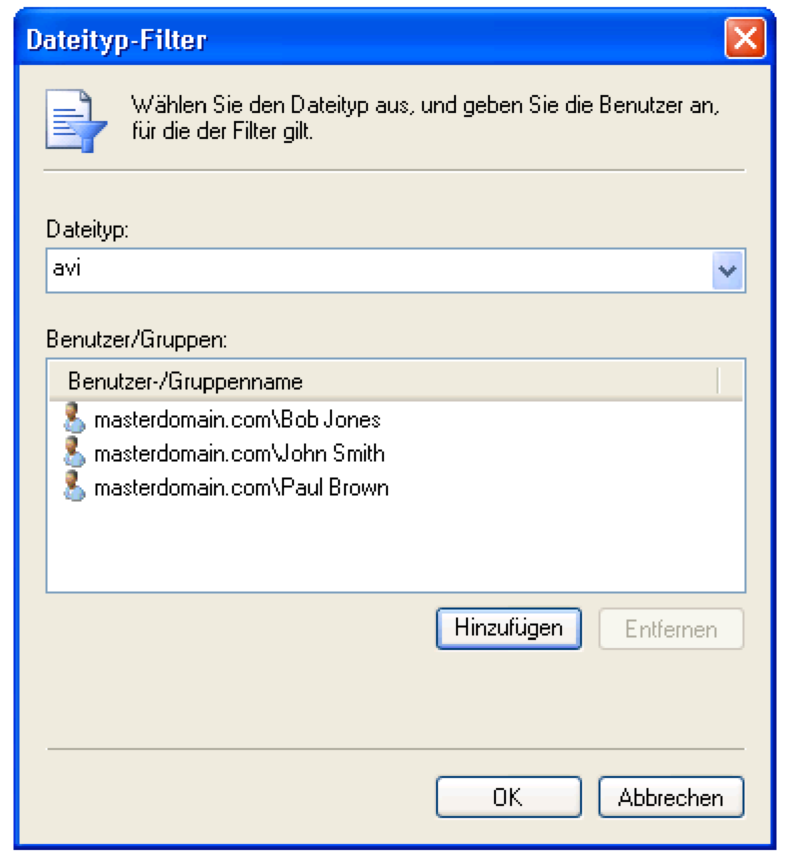



*Screenshot 90 - Optionen für Dateityp-Filter*

5. Wählen Sie im Dialog **Dateityp-Filter** die auf diese Schutzrichtlinie anzuwendende Einschränkung aus:

» Den Zugriff auf alle Dateien gewähren, jedoch die Verwendung der folgenden Dateitypen sperren

» Alle Dateien sperren, jedoch die Verwendung der folgenden Dateitypen gewähren




*Screenshot 91 - Optionen für Dateityp-Filter und Benutzer*

6. Klicken Sie auf **Hinzufügen…**, und wählen Sie den Dateityp aus dem Dropdown-Menü **Dateityp** aus oder geben Sie ihn ein.

7. Klicken Sie auf **Hinzufügen...**, um die Benutzer/Gruppen festzulegen, die auf diesen Dateityp zugreifen können oder dafür gesperrt sind. Klicken Sie anschließend auf **OK**.

Wiederholen Sie die vorherigen 2 Unterschritte für jeden zu beschränkenden Dateityp.

8. Klicken Sie zweimal auf **OK**.

So stellen Sie Aktualisierungen für Schutzrichtlinien auf den von der Schutzrichtlinie kontrollierten Computern bereit:

1. Klicken Sie in der GFI EndPointSecurity-Verwaltungskonsole auf die Registerkarte **Konfiguration**.

2. Klicken Sie auf die untergeordnete Registerkarte **Computer**.

3. Klicken Sie im linken Bereich im Abschnitt **Allgemeine Aufgaben** auf den Hyperlink **Auf allen Computern bereitstellen....**

## 9.14 Konfigurieren der Sicherheitsverschlüsselung

GFI EndPointSecurity bietet Ihnen die Möglichkeit, den Zugriff für Active Directory (AD)-Benutzer und/oder -Benutzergruppen, oder lokale Benutzer und/oder Benutzerschemen auf bestimmte Dateitypen auf Geräten, die mit BitLocker To Go (einer Funktion von Microsoft Windows 7) verschlüsselt wurden, einzuschränken. Diese Einschränkungen werden angewendet, wenn verschlüsselte Geräte an die durch die Schutzrichtlinie kontrollierten Computer angeschlossen werden.

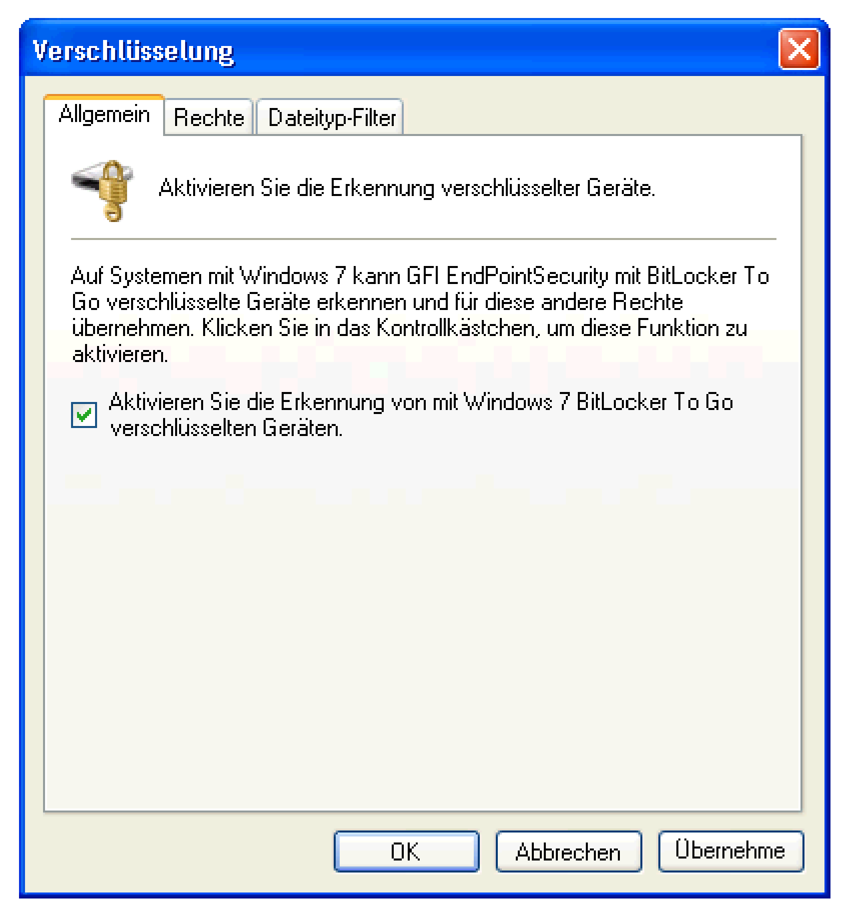
So konfigurieren Sie Einschränkungen für Geräte, die für diese Schutzrichtlinie mit BitLocker To Go verschlüsselt wurden:

1. Klicken Sie in der GFI EndPointSecurity-Verwaltungskonsole auf die Registerkarte **Konfiguration**.

2. Klicken Sie auf die untergeordnete Registerkarte **Schutzrichtlinien**.

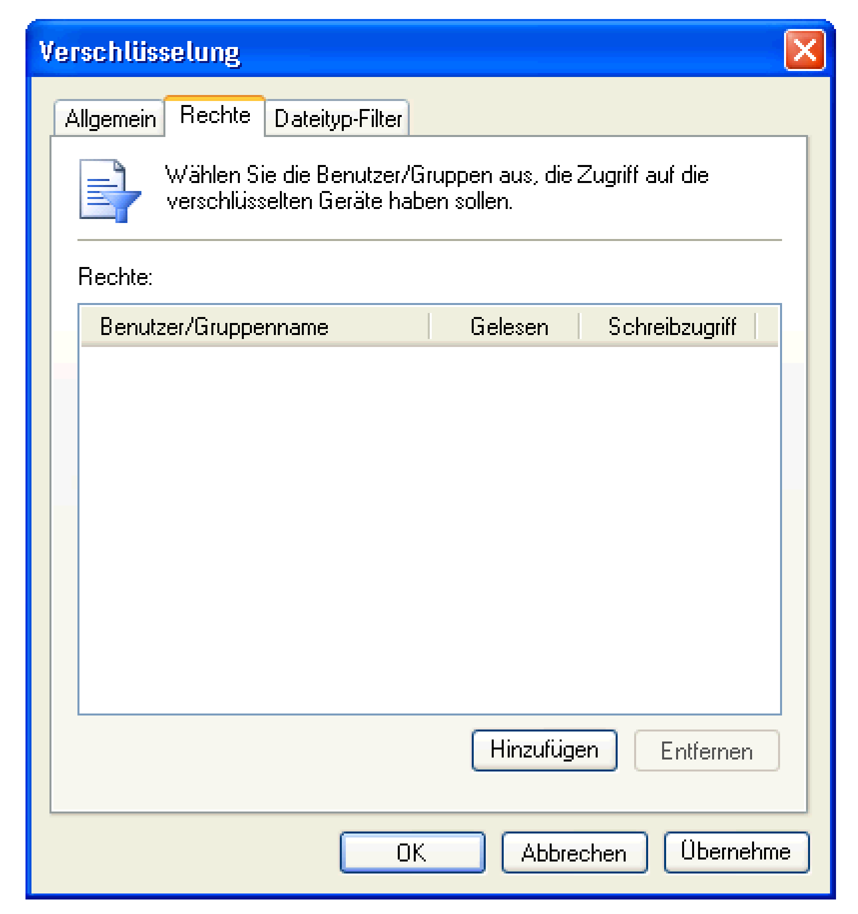
3. Wählen Sie im linken Bereich die Schutzrichtlinie aus, für die Sie Dateitypeinschränkungen definieren möchten.

4. Klicken Sie im rechten Bereich im Abschnitt **Sicherheit** auf den Hyperlink **Verschlüsselung**.




*Screenshot 92 - Verschlüsselungsoptionen - Registerkarte „Allgemein“*

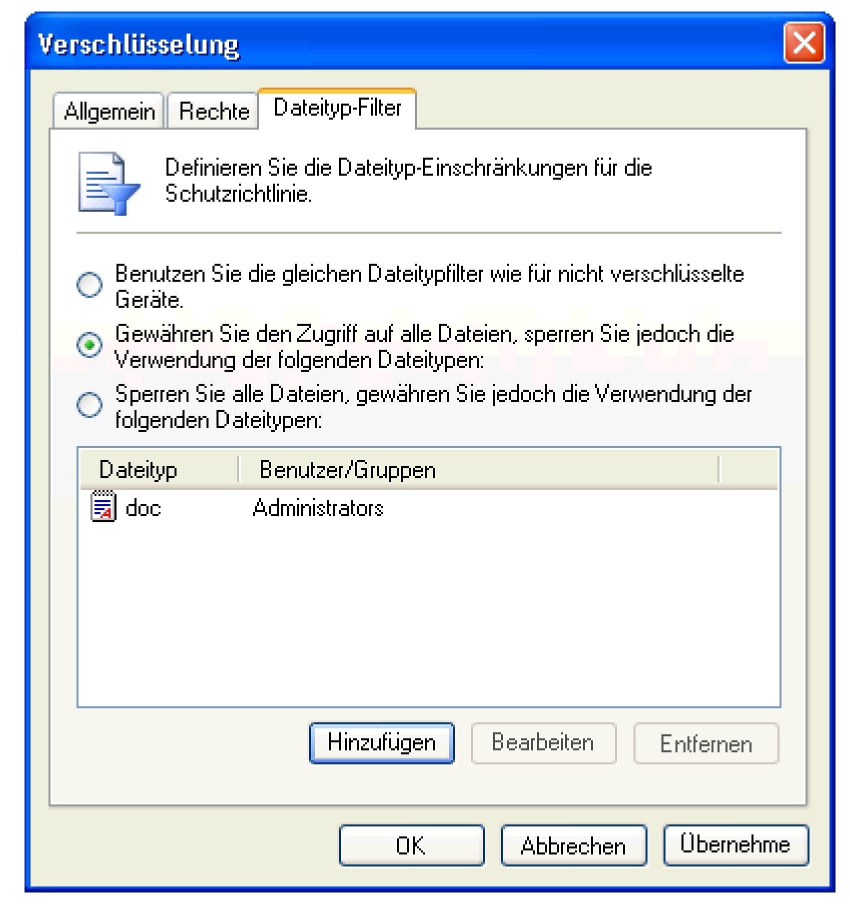
5. Wählen Sie im Dialog **Verschlüsselung** die Registerkarte **Allgemein**, und aktivieren bzw. deaktivieren Sie das Kontrollkästchen **Erkennung von Geräten, die mit Windows 7 BitLocker To Go verschlüsselt wurden, aktivieren**, um die Verwendung von Geräten, die mit BitLocker To Go verschlüsselt wurden, zuzulassen oder zu blockieren.




*Screenshot 93 - Verschlüsselungsoptionen - Registerkarte „Berechtigungen“*

6. Falls die BitLocker To Go-Option aktiviert ist, wechseln Sie auf die Registerkarte **Berechtigungen**.

7. Klicken Sie auf **Hinzufügen**, um die Benutzer/Gruppen festzulegen, die auf diese verschlüsselten Geräte, die von dieser Schutzrichtlinie erkannt wurden, Zugriff haben. Klicken Sie anschließend auf **OK**.




*Screenshot 94 - Verschlüsselungsoptionen - Registerkarte „Dateityp-Filter“*

8. Falls die BitLocker To Go-Option aktiviert ist, wählen Sie die Registerkarte **Dateityp-Filter**, um die zugriffsbeschränkten Dateitypen zu konfigurieren.

9. Wählen Sie die auf diese Schutzrichtlinie anzuwendende Einschränkung aus:

- » Die gleichen Dateityp-Filter für nicht verschlüsselte Geräte verwenden
- » Den Zugriff auf alle Dateien gewähren, jedoch die Verwendung der folgenden Dateitypen sperren
- » Alle Dateien sperren, jedoch die Verwendung der folgenden Dateitypen gewähren

10. Klicken Sie für die letzten beiden Optionen auf **Hinzufügen…**, und wählen Sie den Dateityp aus dem Dropdown-Menü **Dateityp** aus oder geben Sie ihn ein.

11. Klicken Sie auf **Hinzufügen...**, um die Benutzer/Gruppen festzulegen, die auf diesen Dateityp zugreifen können oder dafür gesperrt sind. Klicken Sie anschließend auf **OK**.

Wiederholen Sie die vorherigen 2 Unterschritte für jeden zu beschränkenden Dateityp.

12. Klicken Sie zweimal auf **OK**.

So stellen Sie Aktualisierungen für Schutzrichtlinien auf den von der Schutzrichtlinie kontrollierten Computern bereit:

1. Klicken Sie in der GFI EndPointSecurity-Verwaltungskonsole auf die Registerkarte **Konfiguration**.

2. Klicken Sie auf die untergeordnete Registerkarte **Computer**.

3. Klicken Sie im linken Bereich im Abschnitt **Allgemeine Aufgaben** auf den Hyperlink **Auf allen Computern bereitstellen....**

## 9.15 Konfigurieren der Ereignisprotokollierung

GFI EndPointSecurity-Agenten erfassen auf kontrollierten Computern alle Ereignisse zu Zugriffsversuchen auf Geräte und Schnittstellen. Sie erfassen außerdem dienstspezifische Ereignisse. Sie können festlegen, wo diese Ereignisse gespeichert werden und auch, welche Ereignisarten protokolliert werden. Diese Konfigurierung kann für jede einzelne Richtlinie erfolgen.

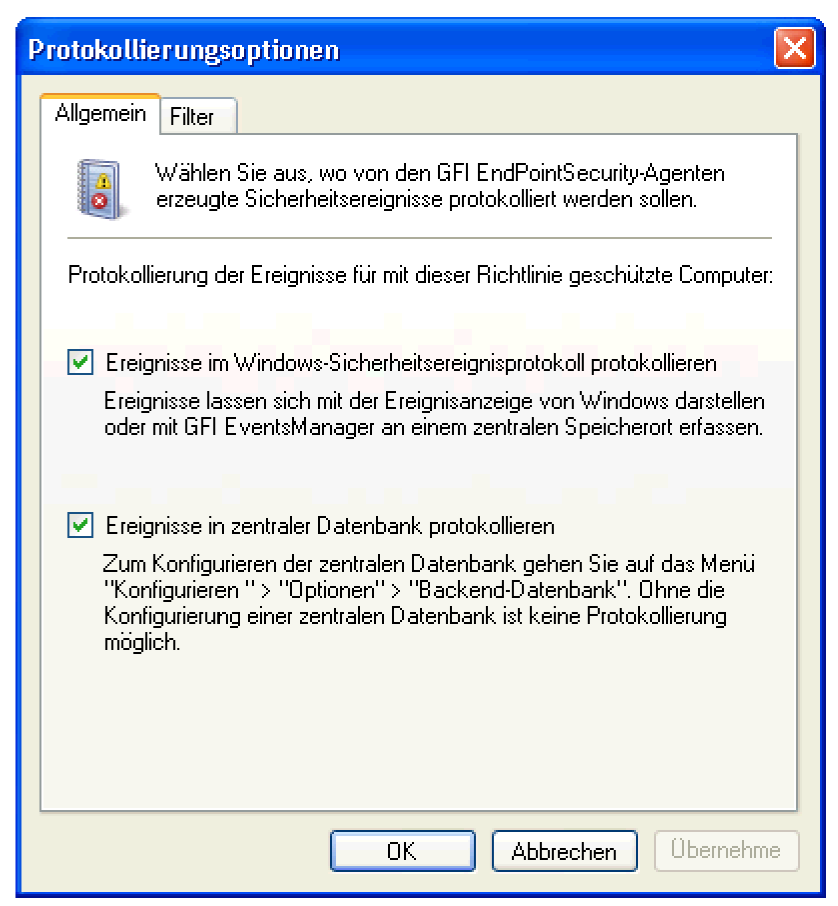
So legen Protokollierungsoptionen für Benutzer innerhalb einer Schutzrichtlinie fest:

1. Klicken Sie in der GFI EndPointSecurity-Verwaltungskonsole auf die Registerkarte **Konfiguration**.

2. Klicken Sie auf die untergeordnete Registerkarte **Schutzrichtlinien**.

3. Wählen Sie im linken Bereich die Schutzrichtlinie aus, für die Sie Protokollierungsoptionen festlegen möchten.

4. Klicken Sie im rechten Bereich im Abschnitt **Protokollierung und Alarme** auf den Hyperlink **Protokollierung und Alarme**.




*Screenshot 95 - Protokollierungsoptionen - Registerkarte „Allgemein“*

5. Wählen Sie im Dialog **Protokollierungsoptionen** die Registerkarte **Allgemein**.

6. Aktivieren bzw. deaktivieren Sie die Speicherorte, an denen von dieser Schutzrichtlinie generierte Ereignisse gespeichert werden sollen.

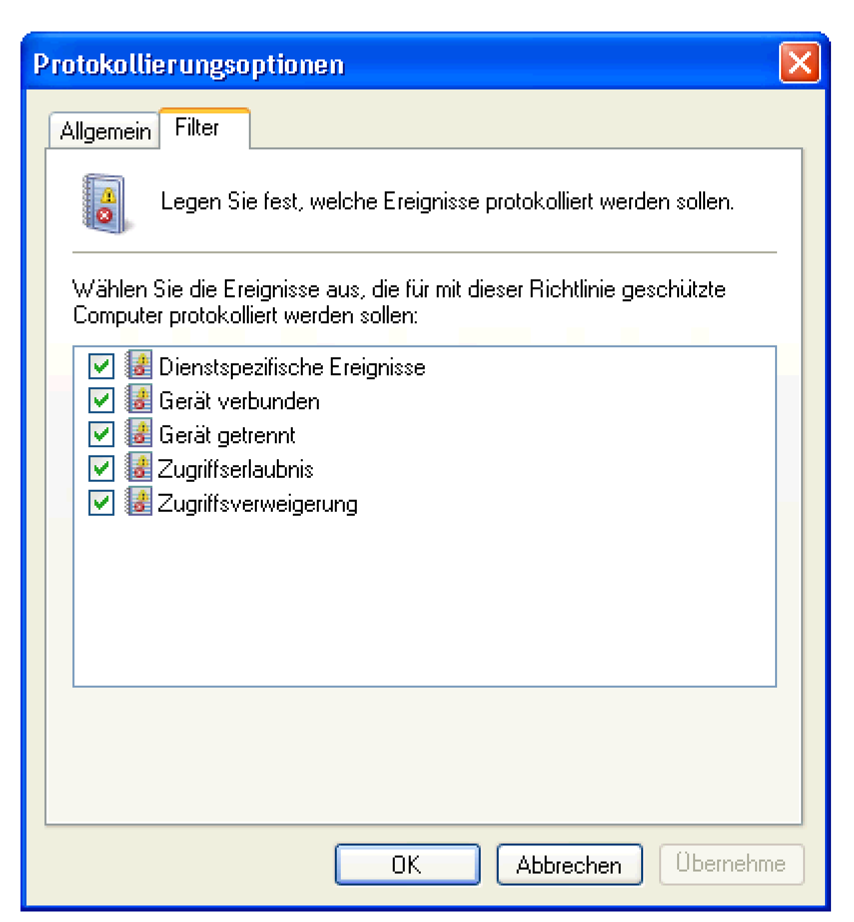
- **Ereignisse im Windows-Sicherheitsereignisprotokoll speichern** – Sie können Ereignisse in der Windows-Ereignisanzeige auf jedem Computer oder über den GFI EventsManager anzeigen, nachdem sie an einer zentralen Stelle gesammelt wurden.

- **Ereignisse in der zentralen Datenbank speichern** – Sie können Ereignisse auf der untergeordneten Registerkarte „Protokoll-Browser“ in der GFI EndPointSecurity-Verwaltungskonsole anzeigen. Diese Option erfordert die Konfiguration einer zentralen Datenbank. Weitere Informationen zur Konfiguration einer zentralen

Datenbank finden Sie im Kapitel Anpassen von GFI EndPointSecurity unter Konfigurieren des Datenbank-Backends.



Falls beide Optionen aktiviert sind, werden die gleichen Daten an beiden Speicherorten protokolliert.




*Screenshot 96 - Protokollierungsoptionen - Registerkarte „Filter“*

7. Wählen Sie auf der Registerkarte **Filter** aus den folgenden Ereignistypen aus, die durch diese Schutzrichtlinie protokolliert werden sollen. Klicken Sie anschließend auf **OK**:

» Dienstereignisse,

» Ereignis - Geräteanschluss,

» Ereignis - Gerätetrennung,

» Ereignis - Zugriffserlaubnis,

» Ereignis - Zugriffsverweigerung.

So stellen Sie Aktualisierungen für Schutzrichtlinien auf den von der Schutzrichtlinie kontrollierten Computern bereit:

1. Klicken Sie in der GFI EndPointSecurity-Verwaltungskonsole auf die Registerkarte **Konfiguration**.

2. Klicken Sie auf die untergeordnete Registerkarte **Computer**.

3. Klicken Sie im linken Bereich im Abschnitt **Allgemeine Aufgaben** auf den Hyperlink **Auf allen Computern bereitstellen...**.

## 9.16 Konfigurieren der Alarme

GFI EndPointSecurity kann so konfiguriert werden, dass bei bestimmten Ereignissen Alarme an festgelegte Empfänger verschickt werden. Sie können die Alarme über verschiedene Warnoptionen konfigurieren und auch die Ereignisarten festlegen, für die Alarme gesendet werden. Diese Konfigurierung kann für jede einzelne Richtlinie erfolgen.



Alarmempfänger sind keine Active Directory (AD)-Benutzer, Benutzergruppen, lokale Benutzer und/oder Benutzerschemen. Es sind von GFI EndPointSecurity erstellte Profilkonten, die Kontaktdetails von Benutzern enthalten, die für Alarme vorgesehen sind. Am besten sollten Alarmempfänger vor der Konfiguration der Alarme erstellt werden. Weitere Informationen zur Erstellung von Benutzern und Gruppen für Benachrichtigungszwecke finden Sie im Kapitel Anpassen von GFI EndPointSecurity unter Konfigurieren der Alarmempfänger.

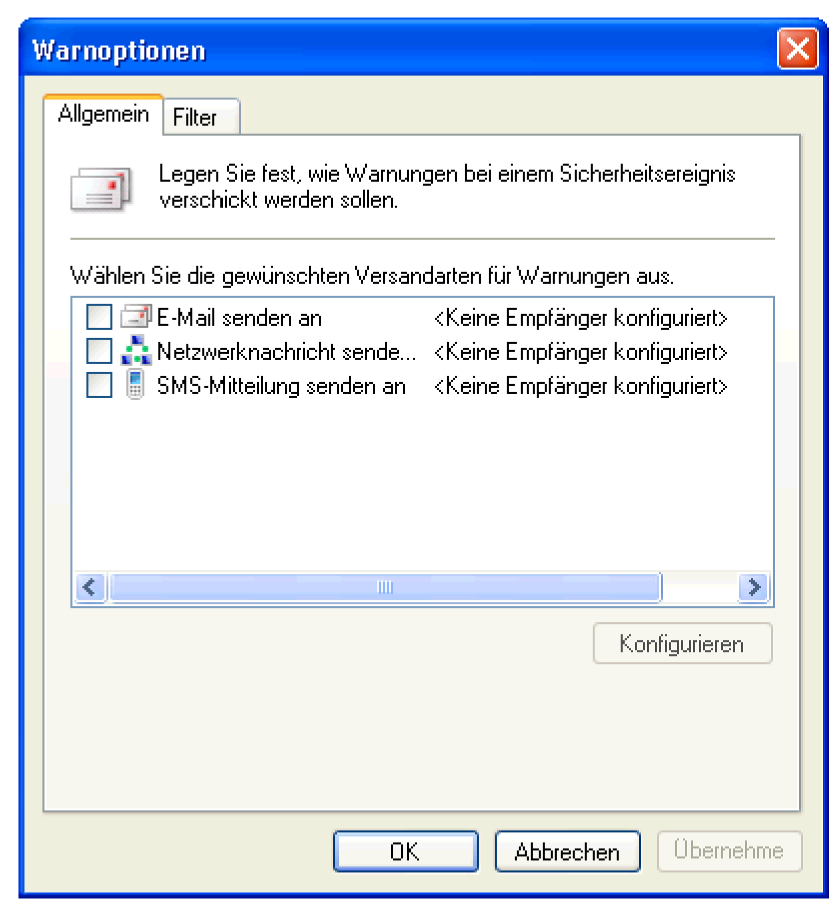
So legen Warnoptionen für Benutzer innerhalb einer Schutzrichtlinie fest:

1. Klicken Sie in der GFI EndPointSecurity-Verwaltungskonsole auf die Registerkarte **Konfiguration**.

2. Klicken Sie auf die untergeordnete Registerkarte **Schutzrichtlinien**.

3. Wählen Sie im linken Bereich die Schutzrichtlinie aus, für die Sie Warnoptionen festlegen möchten.

4. Klicken Sie im rechten Bereich im Abschnitt **Protokollierung und Alarme** auf den Hyperlink **Warnoptionen**.



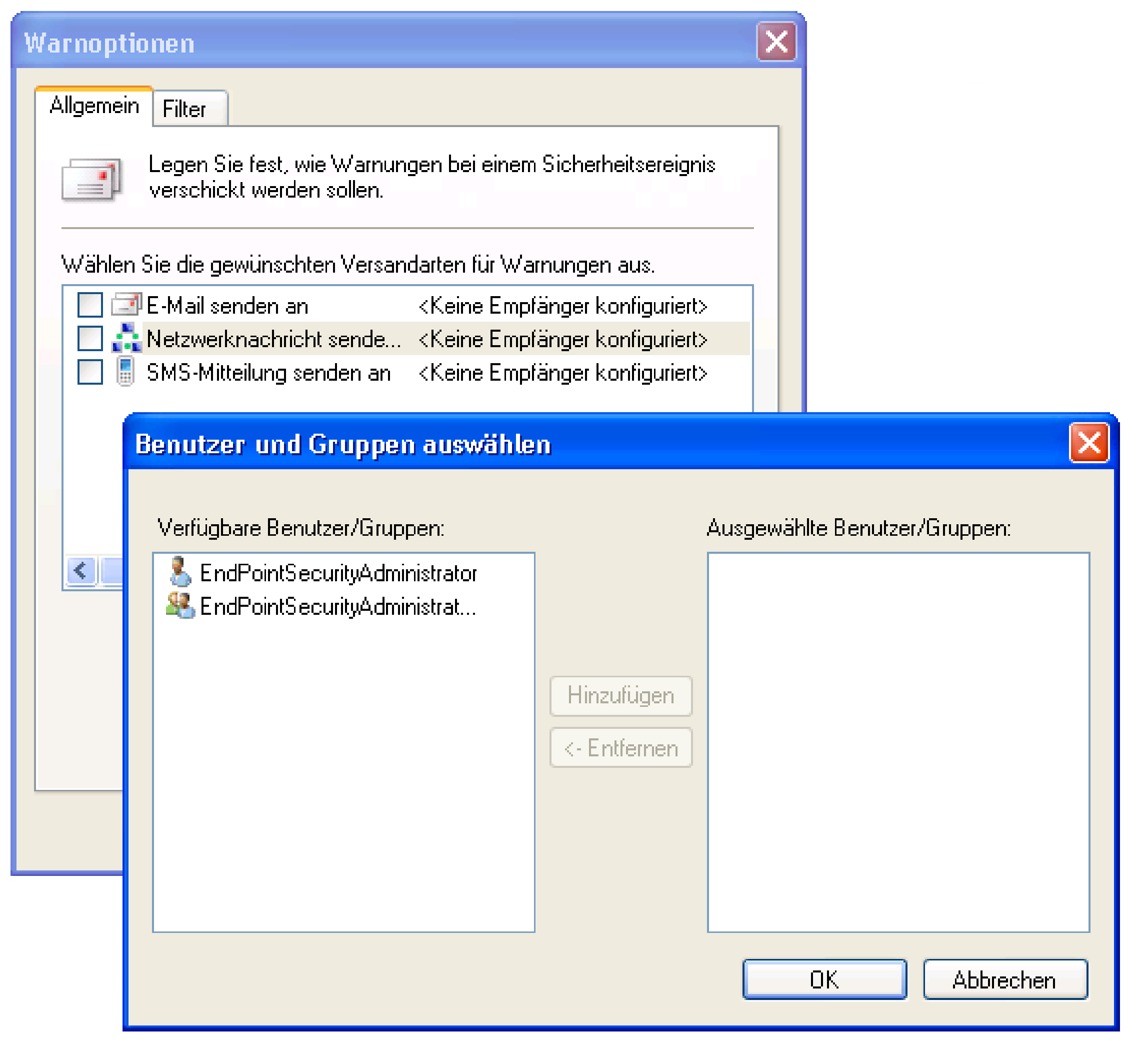

*Screenshot 97 - Warnoptionen - Registerkarte „Allgemein“*

5. Wählen Sie im Dialog **Warnoptionen** die Registerkarte **Allgemein** aus, und wählen Sie die Alarmtypen, die an Alarmempfänger gesendet werden sollen:

- E-Mail-Warnungen,

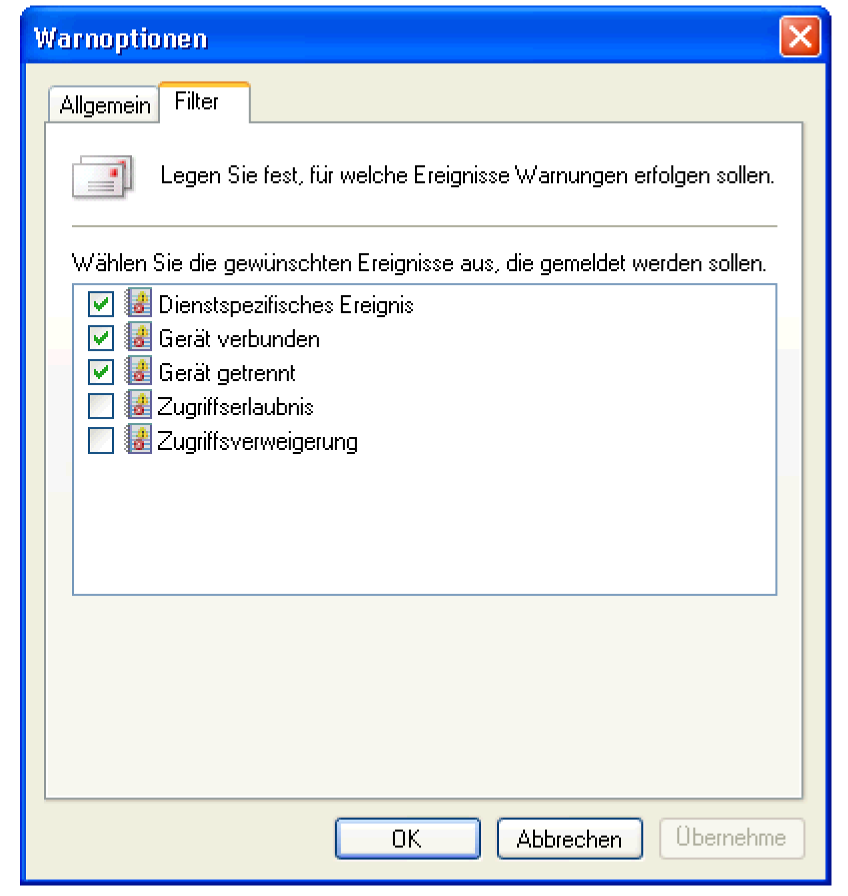
» Netzwerknachrichten,

» SMS-Nachrichten.




*Screenshot 98 - Warnoptionen - Konfigurieren von Benutzern und Gruppen*

6. Markieren Sie für jeden aktivierten Alarm den Alarmtyp, und klicken Sie auf **Konfigurieren**, um die Benutzer/Gruppen festzulegen, an die der Alarm gesendet werden sollen. Klicken Sie anschließend auf **OK**.




*Screenshot 99 - Warnoptionen - Registerkarte „Filter“*

7. Wählen Sie auf der Registerkarte **Filter** aus den folgenden Ereignistypen aus, für die Alarme durch diese Schutzrichtlinie gesendet werden sollen. Klicken Sie anschließend auf **OK**:

» Dienstereignisse,

» Ereignis - Geräteanschluss,

» Ereignis - Gerätetrennung,

» Ereignis - Zugriffserlaubnis,

» Ereignis - Zugriffsverweigerung.

So stellen Sie Aktualisierungen für Schutzrichtlinien auf den von der Schutzrichtlinie kontrollierten Computern bereit:

1. Klicken Sie in der GFI EndPointSecurity-Verwaltungskonsole auf die Registerkarte **Konfiguration**.

2. Klicken Sie auf die untergeordnete Registerkarte **Computer**.

3. Klicken Sie im linken Bereich im Abschnitt **Allgemeine Aufgaben** auf den Hyperlink **Auf allen Computern bereitstellen....**

## 9.17 Festlegen einer Standardrichtlinie

GFI EndPointSecurity gibt Ihnen die Möglichkeit, eine Schutzrichtlinie zu erstellen, die durch die Bereitstellungsfunktion neu erkannten Computern zugewiesen wird. Diese Konfigurierung kann für jede einzelne Richtlinie erfolgen.

Standardmäßig geschieht Folgendes:

» Die Bereitstellungsfunktion ist so konfiguriert, dass sie die Standardschutzrichtlinie **Allgemeine Kontrolle** verwendet. Sie können jedoch auch eine andere Richtlinie als Standard festlegen.

So legen Sie eine andere Schutzrichtlinie als Standard fest:

1. Klicken Sie in der GFI EndPointSecurity-Verwaltungskonsole auf die Registerkarte **Konfiguration**.

2. Klicken Sie auf die untergeordnete Registerkarte **Schutzrichtlinien**.

3. Wählen Sie im linken Bereich die Schutzrichtlinie aus, die Sie als Standard festlegen möchten.

4. Klicken Sie im linken Bereich im Abschnitt **Allgemeine Aufgaben** auf den Hyperlink **Als Standardrichtlinie festlegen**.

# 10 Anpassen von GFI EndPointSecurity

## 10.1 Einführung

Alle Einstellungen innerhalb von GFI EndPointSecurity sind komplett benutzerdefinierbar und können vollständig an die unternehmensspezifischen Bedürfnisse angepasst werden. In diesem Kapitel werden folgende Aspekte behandelt:

- Konfigurieren der automatischen Suche
- Konfigurieren des Administratorkontos für Alarme
- Konfigurieren der Warnoptionen
- Konfigurieren der Alarmempfänger
- Konfigurieren von Alarmempfängergruppen
- Konfigurieren des Übersichtsberichts
- Konfigurieren des Datenbank-Backends
- Konfigurieren von Benutzerbenachrichtigungen
- Konfigurieren von erweiterten Optionen.

## 10.2 Konfigurieren der automatischen Suche

GFI EndPointSecurity ermöglicht mithilfe der automatischen Suche die zeitgesteuerte Suche nach neu angeschlossenen Computern im Netzwerk. Dafür können folgende Einstellungen konfiguriert werden:

- Häufigkeit und der Zeitplan der Suchen,
- Abgedeckter Erkennungsbereich,
- Richtlinie, die neu erkannten Computern zugewiesen wird, und Anmeldeinformationen.

Standardmäßig geschieht Folgendes:

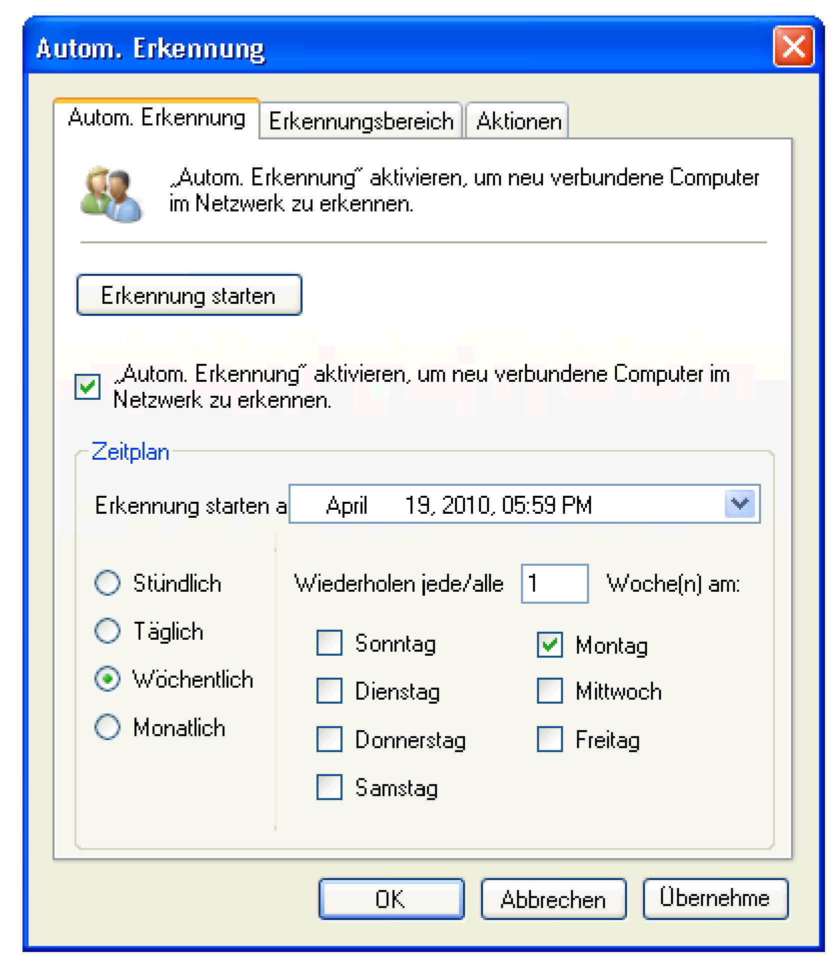
- Die automatische Suche ist so konfiguriert, dass die **Aktuelle Domäne/Arbeitsgruppe** durchsucht wird.
- Die Installationseinstellungen sind so konfiguriert, dass die Standardschutzrichtlinie **Allgemeine Kontrolle** neu erkannten Computern zugewiesen wird.

So konfigurieren Sie die automatische Suche:

1. Klicken Sie in der GFI EndPointSecurity-Verwaltungskonsole auf die Registerkarte **Konfiguration**.

2. Klicken Sie auf die untergeordnete Registerkarte **Computer**.

3. Klicken Sie im linken Bereich im Abschnitt **Allgemeine Aufgaben** auf den Hyperlink **Einstellungen für autom. Suche**.



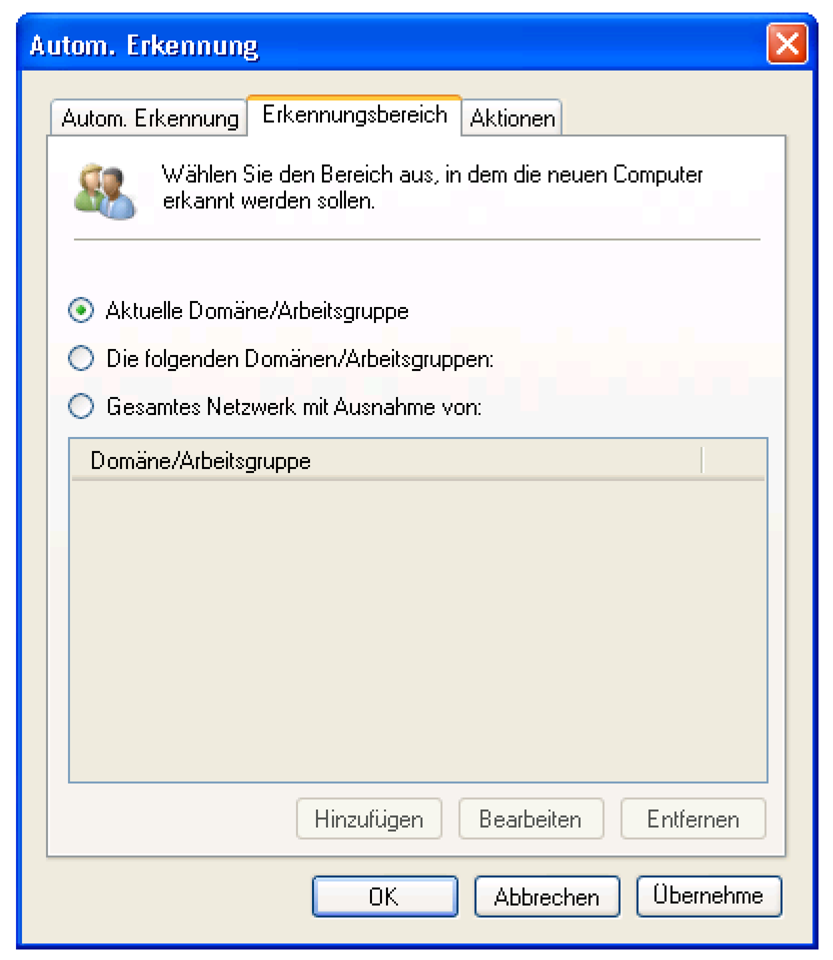

*Screenshot 100 - Optionen für die automatische Suche - Registerkarte „Automatische Suche"*

4. Wählen Sie im Dialog **Automatische Suche** die Registerkarte **Automatische Suche**.

5. Klicken Sie auf **Suche jetzt starten**, um die automatische Suche auszuführen.

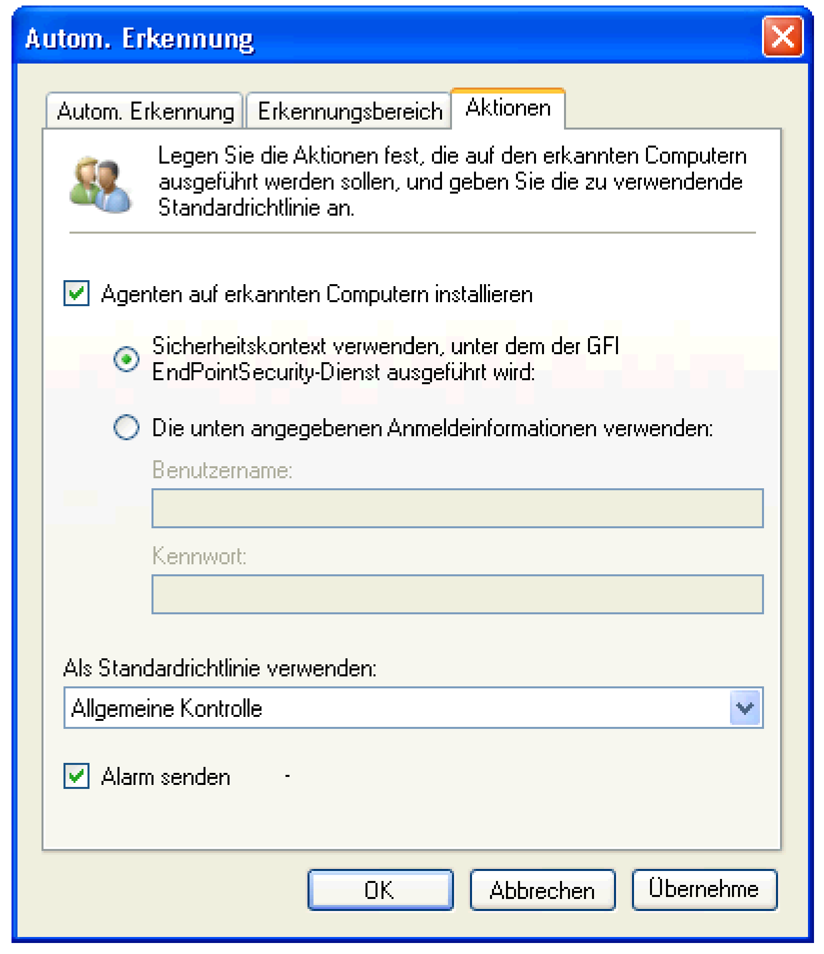
6. Aktivieren oder deaktivieren Sie das Kontrollkästchen **Automatische Suche aktivieren, um neue Computer im Netzwerk zu finden**.

7. Wählen Sie im Bereich **Zeitplan** das Startdatum und die Häufigkeit der Suchen mit den Optionen **Stündlich**, **Täglich**, **Wöchentlich** oder **Monatlich** aus.




*Screenshot 101 - Optionen für die automatische Suche - Registerkarte „Erkennungsbereich“*

8. Wechseln Sie auf die Registerkarte **Erkennungsbereich**, und wählen Sie den zu durchsuchenden Bereich aus. Klicken Sie für die Optionen **Die folgenden Domänen/Arbeitsgruppen** und **Gesamtes Netzwerk außer** auf **Hinzufügen**, und geben Sie den **Namen der Domäne/Arbeitsgruppe** ein.




*Screenshot 102 - Optionen für die automatische Suche - Registerkarte „Aktionen“*

9. Wählen Sie die Registerkarte **Aktionen**, und aktivieren oder deaktivieren Sie die Option **Agenten auf erkannten Computern installieren.** Klicken Sie bei Aktivierung auf **Ja**, um die Aktivierung des Automatischen Schutzes zu bestätigen. Wählen Sie die Anmeldeninformationen, die GFI EndPointSecurity für die physikalische Anmeldung auf den zu überwachenden Computern benötigt.



GFI EndPointSecurity verwendet standardmäßig die Anmeldeinformationen des aktuell angemeldeten Benutzers, unter dem die GFI EndPointSecurity ausgeführt wird.

10. Wählen Sie die Schutzrichtlinie aus dem Dropdown-Menü aus, die automatisch auf neu erkannten Computern angewendet werden soll.

11. Aktivieren oder deaktivieren Sie die Option **Alarm senden**, und klicken Sie auf **OK**.

## 10.3 Konfigurieren des Administratorkontos für Alarme

GFI EndPointSecurity gibt Ihnen die Möglichkeit, Profilkonten zu konfigurieren, die die Kontaktdetails von Benutzern enthalten. Diese Benutzer sind dafür vorgesehen, E-Mail-Warnungen und Netzwerk- bzw. SMS-Nachrichten zu erhalten. Nach der Installation erstellt GFI EndPointSecurity automatische ein Administratorkonto für Alarme ohne die folgenden Kontaktdetails:

- Kontaktdaten wie E-Mail-Adresse und Telefonnummer
- Kernarbeitszeit,
- Art der während und außerhalb der Kernarbeitszeit zu verschickenden Alarme,
- Benachrichtigungsgruppe, zu der der Benutzer gehört.



Alarmadministratoren sind keine Active Directory (AD)-Benutzer und/oder -Benutzergruppen, oder lokale Benutzern und/oder Benutzerschemen.

Standardmäßig geschieht Folgendes:

» GFI EndPointSecurity erstellt nach der Installation automatisch das Konto **EndPointSecurityAdministrator** (für Alarme) und legt es als Mitglied der Benachrichtigungsgruppe **EndPointSecurityAdministratoren** fest.

So konfigurieren Sie das GFI EndPointSecurityAdministrator-Konto:

1. Klicken Sie in der GFI EndPointSecurity-Verwaltungskonsole auf die Registerkarte **Konfiguration**.

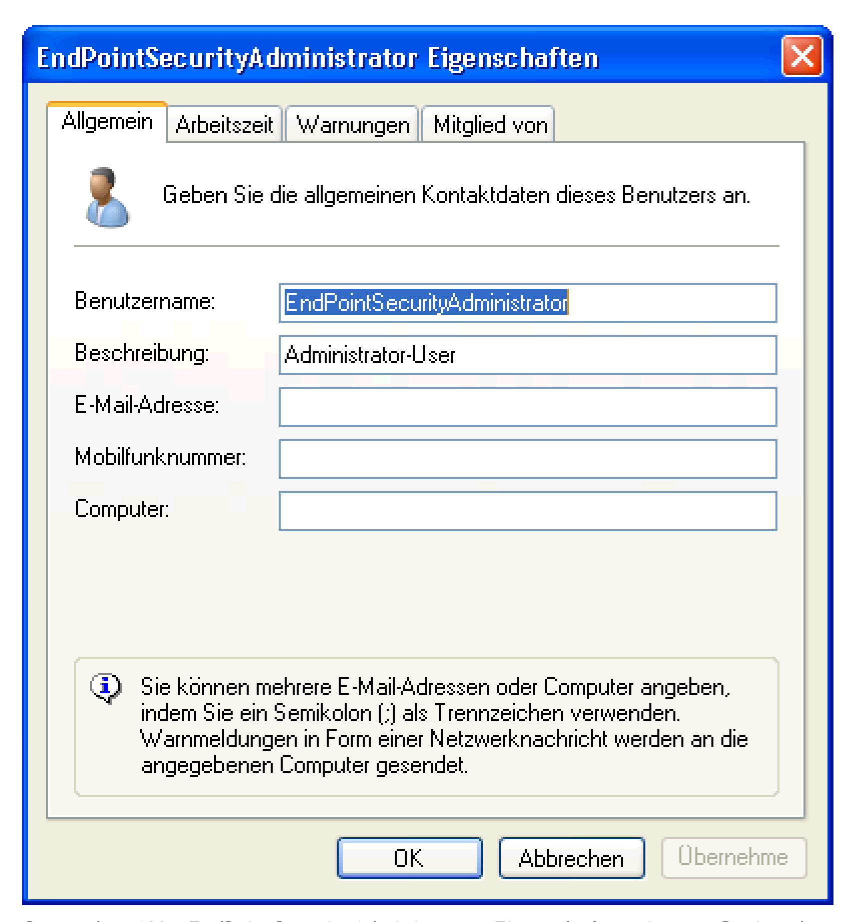
2. Klicken Sie auf die untergeordnete Registerkarte **Optionen**.

3. Klicken Sie auf den Knoten **Warnoptionen**.

4. Klicken Sie auf den Unterknoten **Benutzer**.

5. Markieren Sie im rechten Bereich das Konto **EndPointSecurityAdministrator**.

6. Klicken Sie im linken Bereich im Abschnitt **Aktionen** auf den Hyperlink **Ausgewählten Benutzer bearbeiten....**

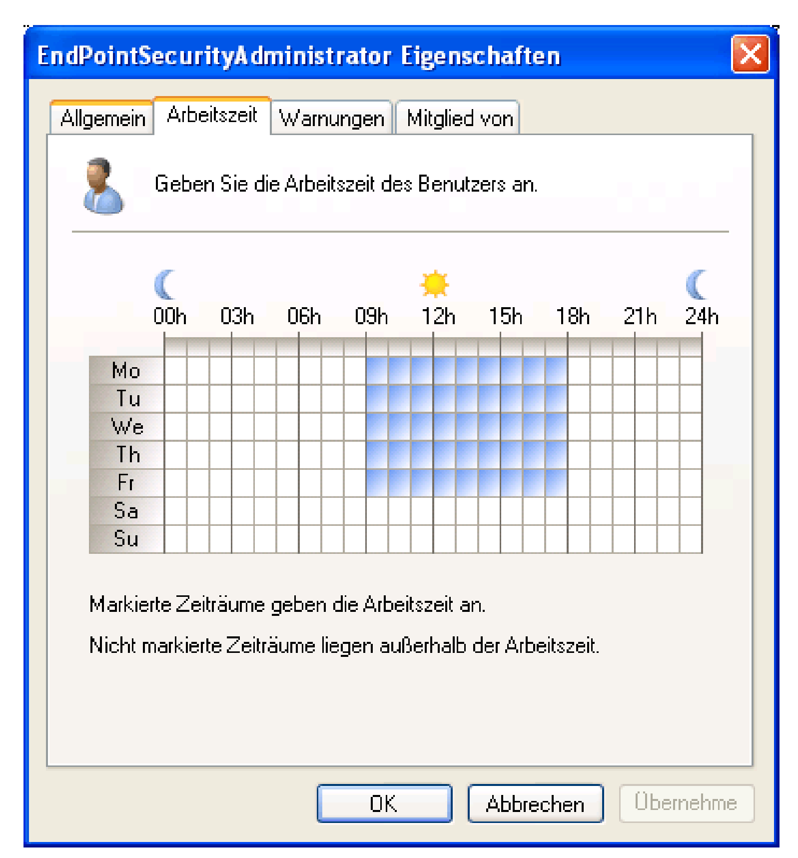



*Screenshot 103 - EndPointSecurityAdministrator-Eigenschaftsoptionen - Registerkarte „Allgemein“*

7. Wählen Sie im Dialog **EndPointSecurityAdministrator-Eigenschaften** die Registerkarte **Allgemein**, und geben Sie als Kontaktdetails die E-Mail-Adressen, Mobiltelefonnummern und Computernamen/IP-Adressen (für Netzwerknachrichten an den Administrator) wie erforderlich ein.

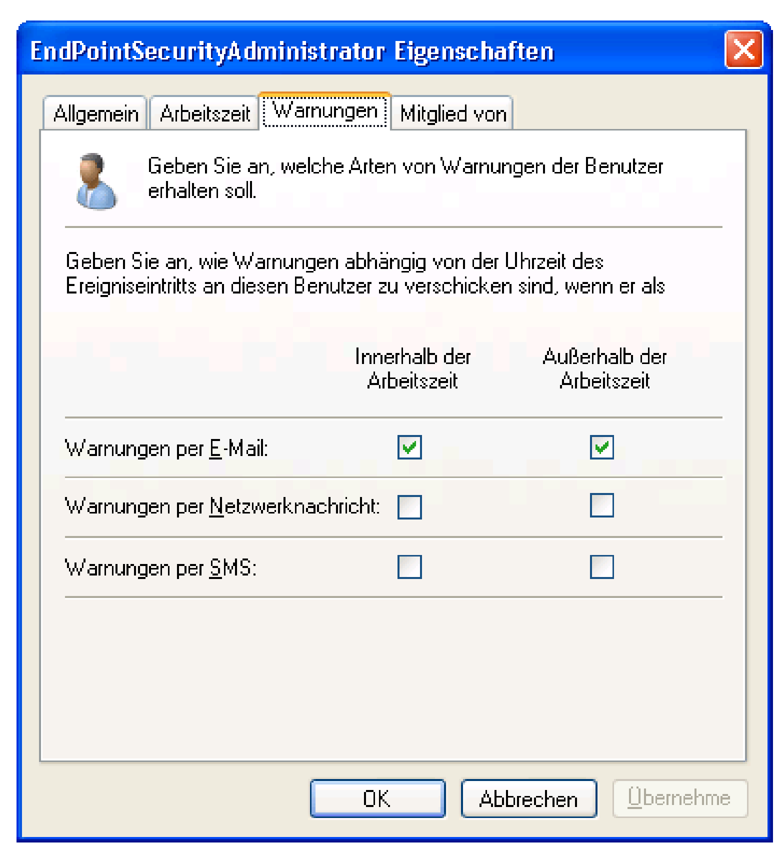


Es können mehrere E-Mail-Adressen und Computernamen/IP-Adressen angegeben werden. Diese müssen dann jeweils mit einem Semikolon (;) von einander getrennt sein.



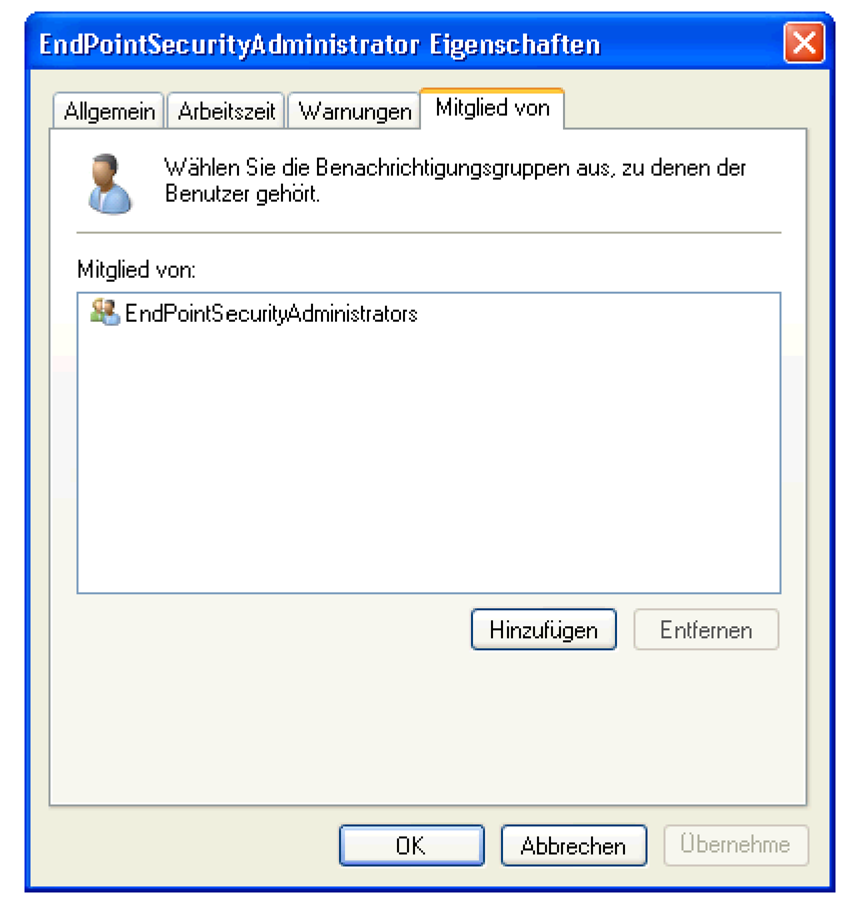

*Screenshot 104 - EndPointSecurityAdministrator-Eigenschaftsoptionen - Registerkarte „Arbeitszeit“*

8. Wählen Sie die Registerkarte **Arbeitszeit**, und markieren Sie die Kernarbeitszeit des Benutzers.




*Screenshot 105 - EndPointSecurityAdministrator-Eigenschaftsoptionen - Registerkarte „Alarme“*

9. Wählen Sie die Registerkarte **Alarme**, und aktivieren Sie Art der Alarme, die während und außerhalb der markierten Arbeitszeit gesendet werden sollen.




*Screenshot 106 - EndPointSecurityAdministrator-Eigenschaftsoptionen - Registerkarte „Mitglied von“*

10. Wählen Sie die Registerkarte **Mitglied von**.

11. Klicken Sie auf **Hinzufügen**, um die Benachrichtigungsgruppe(n) des Benutzers auszuwählen. Klicken Sie anschließend auf **OK**.

## 10.4 Konfigurieren der Warnoptionen

Mit GFI EndPointSecurity können Sie folgende Warnoptionen konfigurieren:

- » Mailserver-Einstellungen, Absenderdetails und die E-Mail-Nachricht, die als E-Mail-Warnung gesendet werden soll,
- » Netzwerknachrichten, die als Netzwerkwarnung gesendet werden soll,
- » SMS-Gateway und SMS-Nachricht, die als SMS-Warnung gesendet werden soll.

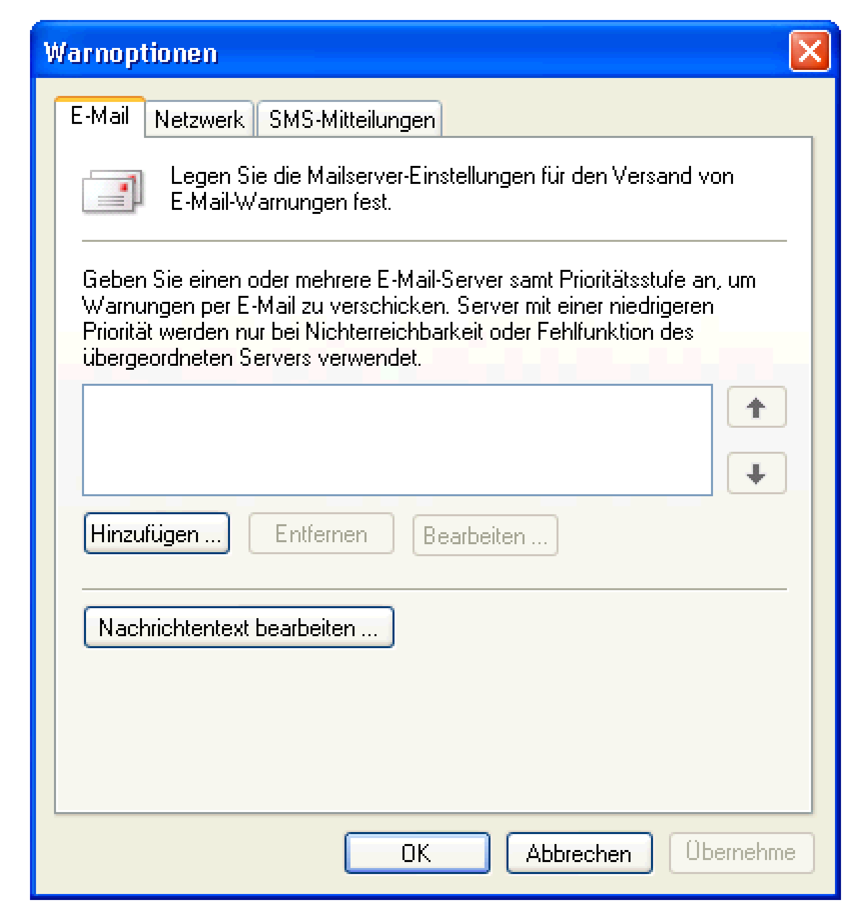
So konfigurieren Sie die allgemeinen Warnparameter:

1. Klicken Sie in der GFI EndPointSecurity-Verwaltungskonsole auf die Registerkarte **Konfiguration**.

2. Klicken Sie auf die untergeordnete Registerkarte **Optionen**.

3. Klicken Sie auf den Knoten **Warnoptionen**.

4. Klicken Sie im rechten Bereich im Abschnitt **Warnoptionen** auf den Hyperlink **Warnoptionen bearbeiten**.

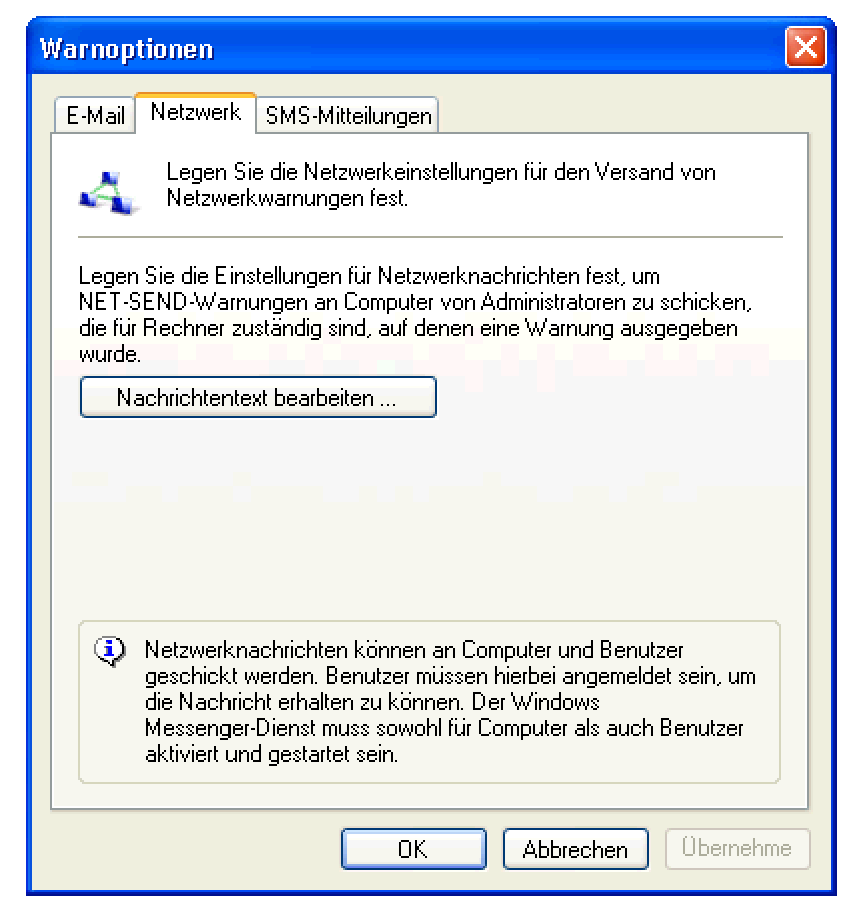



*Screenshot 107 - Warnoptionen - Registerkarte „E-Mail“*

5. Wählen Sie im Dialog **Warnoptionen** die Registerkarte **E-Mail**.

6. Klicken Sie auf **Hinzufügen...**, und geben Sie die Daten für Mail-Server, Authentifizierung (falls erforderlich) und Absender ein. Klicken Sie anschließend auf **OK**.

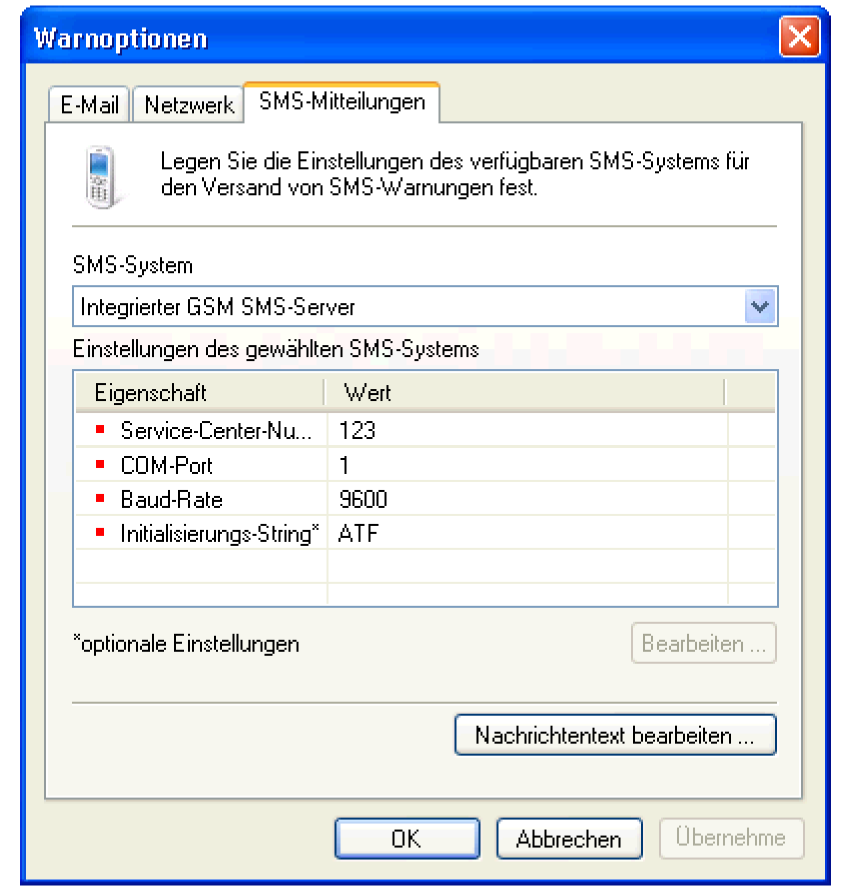
7. Um die E-Mail-Nachricht zu bearbeiten, klicken Sie auf **Nachrichtentext bearbeiten...**, ändern Sie die Felder **Betreff** und **Nachricht**, und klicken Sie auf **Speichern**.




*Screenshot 108 - Warnoptionen - Registerkarte „Netzwerk“*

8. Wählen Sie die Registerkarte **Netzwerk**.

9. Um die Netzwerknachricht zu bearbeiten, klicken Sie auf **Nachrichtentext bearbeiten...**, ändern Sie die Felder **Betreff** und **Nachricht**, und klicken Sie auf **Speichern**.




*Screenshot 109 - Warnoptionen - Registerkarte „SMS"*

10. Wählen Sie die Registerkarte **SMS**.

11. Wählen Sie aus dem Dropdown-Menü das SMS-System aus, über das die SMS-Benachrichtigungen gesendet werden sollen. Unterstützte SMS-Systeme sind:

» GFI FAXmaker-SMS-Gateway,

» E-Mail-zu-SMS-Gateway Clickatell.

12. Markieren Sie in der Liste die zu konfigurierende SMS-Systemeigenschaft, klicken Sie auf **Bearbeiten…**, und ändern Sie gegebenenfalls das Feld **Wert**. Klicken Sie anschließend auf **OK**.

Wiederholen Sie den vorherigen Unterschritt für jede SMS-Systemeigenschaft, die Sie ändern möchten.

13. Um die SMS-Nachricht zu bearbeiten, klicken Sie auf **Nachrichtentext bearbeiten...**, ändern Sie die Felder **Betreff** und **Nachricht**, und klicken Sie auf **Speichern**.

14. Klicken Sie auf **OK**.

## 10.5 Konfigurieren der Alarmempfänger

GFI EndPointSecurity gibt Ihnen die Möglichkeit, andere Profilkonten als das GFI EndPointSecurityAdministrator-Konto zu konfigurieren, um Kontaktdetails von Benutzern zu speichern, die E-Mail-Warnungen, Netzwerknachrichten und SMS-Nachrichten erhalten sollen.

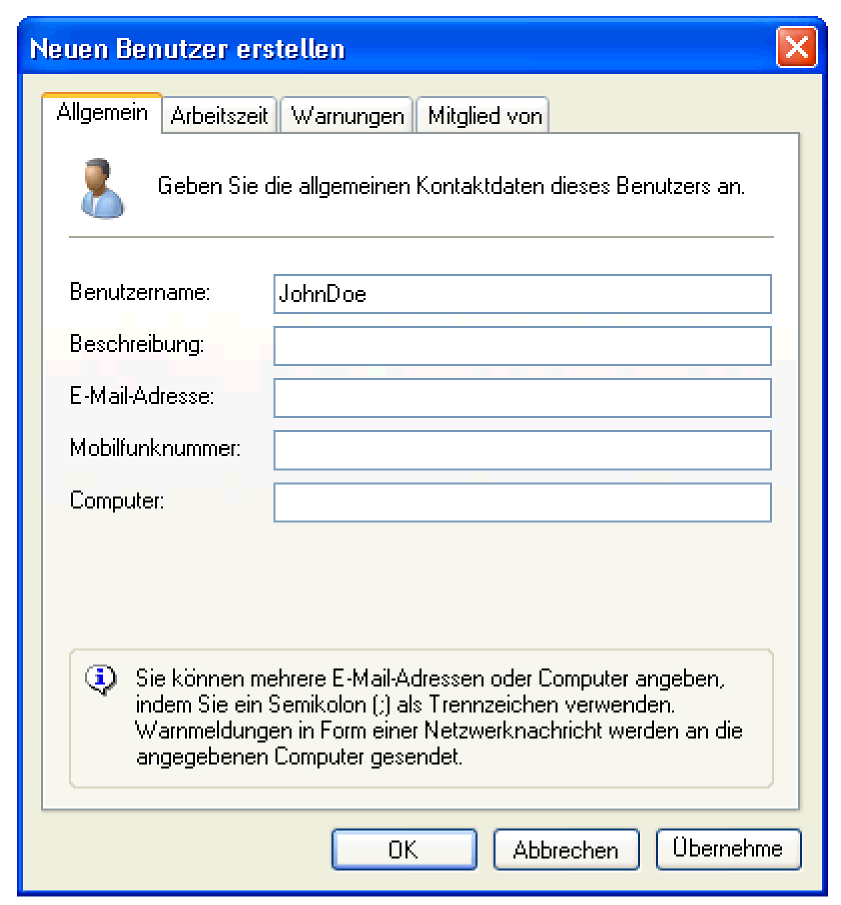


Alarmempfänger sind keine Active Directory (AD)-Benutzer, Benutzergruppen, lokale Benutzer und/oder Benutzerschemen. Es sind von GFI EndPointSecurity erstellte Profilkonten, die Kontaktdetails von Benutzern enthalten, die für Alarme vorgesehen sind.

### 10.5.1 Erstellen von Alarmempfängern

So erstellen Sie einen neuen Alarmempfänger:

1. Klicken Sie in der GFI EndPointSecurity-Verwaltungskonsole auf die Registerkarte **Konfiguration**.
2. Klicken Sie auf die untergeordnete Registerkarte **Optionen**.
3. Klicken Sie auf den Knoten **Warnoptionen**.
4. Klicken Sie auf den Unterknoten **Benutzer**.
5. Klicken Sie im linken Bereich im Abschnitt **Allgemeine Aufgaben** auf den Hyperlink **Benutzer erstellen....**




*Screenshot 110 - Optionen „Neuen Benutzer erstellen“ - Registerkarte „Allgemein“*



Weitere Informationen zur Eingabe der Inhalte im Dialog **Neuen Benutzer erstellen** finden Sie in diesem Kapitel unter **Konfigurieren des Administratorkontos für Alarme**.

6. Klicken Sie auf **OK**.

### 10.5.2 Bearbeiten der Alarmempfängereigenschaften

So bearbeiten Sie der Alarmempfängereigenschaften:

1. Klicken Sie in der GFI EndPointSecurity-Verwaltungskonsole auf die Registerkarte **Konfiguration**.
2. Klicken Sie auf die untergeordnete Registerkarte **Optionen**.
3. Klicken Sie auf den Knoten **Warnoptionen**.
4. Klicken Sie auf den Unterknoten **Benutzer**.
5. Markieren Sie im rechten Bereich das gewünschte Alarmempfängerkonto.

6. Klicken Sie im linken Bereich im Abschnitt **Aktionen** auf den Hyperlink **Ausgewählten Benutzer bearbeiten....**



Weitere Informationen zur Bearbeitung der Inhalte im Dialog für Alarmempfängereigenschaften finden Sie in diesem Kapitel unter Konfigurieren des Administratorkontos für Alarme.

7. Klicken Sie auf **OK**.

### 10.5.3 Löschen von Alarmempfängern

So löschen Sie einen Alarmempfänger:

1. Klicken Sie in der GFI EndPointSecurity-Verwaltungskonsole auf die Registerkarte **Konfiguration**.
2. Klicken Sie auf die untergeordnete Registerkarte **Optionen**.
3. Klicken Sie auf den Knoten **Warnoptionen**.
4. Klicken Sie auf den Unterknoten **Benutzer**.
5. Markieren Sie im rechten Bereich das gewünschte Alarmempfängerkonto.
6. Klicken Sie im linken Bereich im Abschnitt **Aktionen** auf den Hyperlink **Ausgewählten Benutzer löschen...**, und bestätigen Sie mit **Ja**.

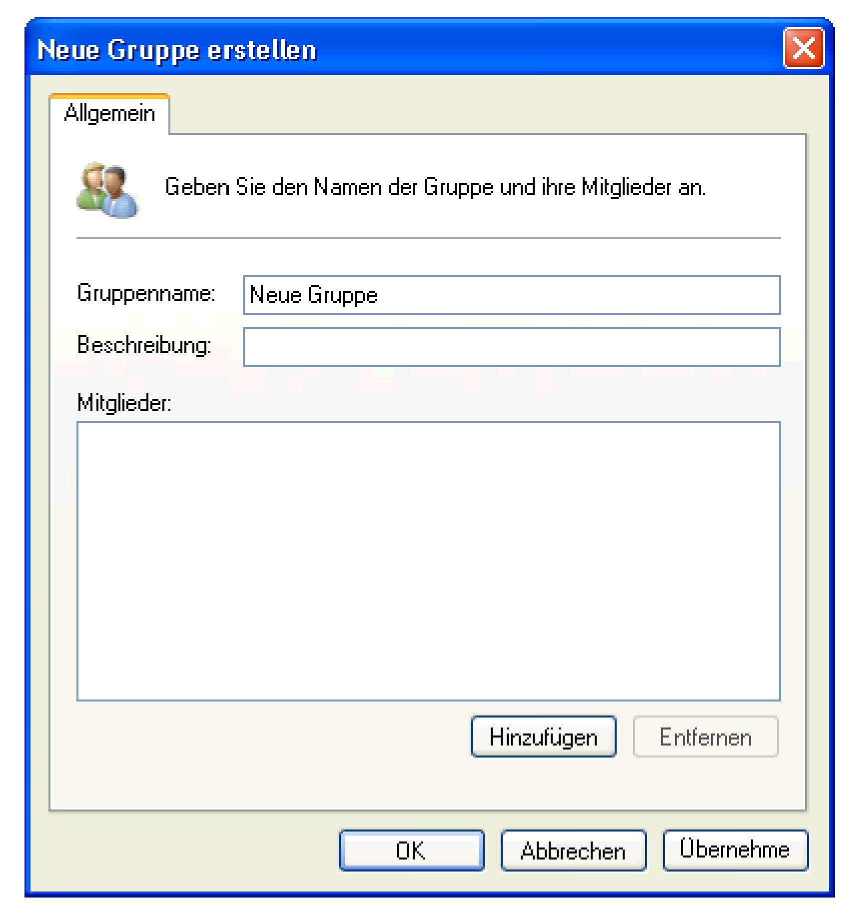
## 10.6 Konfigurieren der Gruppen von Warnungsempfängern

GFI EndPointSecurity ermöglicht die Einteilung Ihrer Warnungsempfänger in Gruppen, um die Verwaltung der Warnungsempfänger zu vereinfachen.

### 10.6.1 Erstellen der Gruppen von Warnungsempfängern

So erstellen Sie eine neue Gruppe von Warnungsempfängern:

1. Klicken Sie in der GFI EndPointSecurity-Verwaltungskonsole auf die Registerkarte **Konfiguration**.
2. Klicken Sie auf die untergeordnete Registerkarte **Optionen**.
3. Klicken Sie auf den Knoten **Warnoptionen**.
4. Klicken Sie auf den Unterknoten **Gruppen**.
5. Klicken Sie im linken Bereich unter **Allgemeine Aufgaben** auf den Hyperlink **Gruppe erstellen....**




*Screenshot 111 - Optionen für das Erstellen neuer Gruppen*

6. Geben Sie im Dialog **Neue Gruppe erstellen** den **Gruppennamen** und bei Bedarf eine **Beschreibung** ein.

7. Klicken Sie auf **Hinzufügen**, um den/die zur Benachrichtigungsgruppe gehörenden Benutzer auszuwählen, und klicken Sie anschließend auf **OK**.

### 10.6.2 Bearbeiten von Eigenschaften einer Gruppe von Warnungsempfängern

So bearbeiten Sie die Eigenschaften für eine Gruppe von Warnungsempfängern:

1. Klicken Sie in der GFI EndPointSecurity-Verwaltungskonsole auf die Registerkarte **Konfiguration**.

2. Klicken Sie auf die untergeordnete Registerkarte **Optionen**.

3. Klicken Sie auf den Knoten **Warnoptionen**.

4. Klicken Sie auf den Unterknoten **Gruppen**.

5. Markieren Sie im rechten Bereich die zu bearbeitende Gruppe.

6. Klicken Sie im linken Bereich unter **Aktionen** auf den Hyperlink **Ausgewählte Gruppe bearbeiten...**.



Weitere Informationen zum Bearbeiten von Gruppeninhalten im Eigenschaftendialog der Warnungsempfänger finden Sie im Abschnitt Erstellen der Gruppen von Warnungsempfängern in diesem Kapitel.

7. Klicken Sie auf **OK**.

### 10.6.3 Löschen der Gruppen von Warnungsempfängern

So löschen Sie eine Gruppe von Warnungsempfängern:

1. Klicken Sie in der GFI EndPointSecurity-Verwaltungskonsole auf die Registerkarte **Konfiguration**.

2. Klicken Sie auf die untergeordnete Registerkarte **Optionen**.

3. Klicken Sie auf den Knoten **Warnoptionen**.

4. Klicken Sie auf den Unterknoten **Gruppen**.

5. Markieren Sie im rechten Bereich die zu löschende Gruppe.

6. Klicken Sie im linken Bereich unter **Aktionen** auf den Hyperlink **Ausgewählte Gruppe löschen**, und klicken Sie anschließend auf **Ja**.

## 10.7 Konfigurieren des Übersichtsberichts

GFI EndPointSecurity ermöglicht mithilfe der folgenden Optionen das Erstellen eines Zusammenfassungsberichts, der die von GFI EndPointSecurity erkannten Aktivitätsstatistiken enthält:

» an Warnungsempfänger zu sendende Warnmeldungen

» Inhalt des Berichts

» Häufigkeit des Berichts



Warnungsempfänger sind weder Active Directory (AD)-Benutzer und/oder -Benutzergruppen noch lokale Benutzer und/oder Gruppen. Sie stellen von GFI EndPointSecurity erstellte Profilkonten dar, die die Kontaktdaten der Benutzer enthalten, die Warnmeldungen erhalten sollen. Warnungsempfänger sollten vor der Warnmeldungskonfiguration erstellt werden. Weitere Informationen zum Erstellen von zu benachrichtigenden Benutzern und Gruppen finden Sie im Abschnitt **Konfigurieren der Alarmempfänger** im Kapitel **Anpassen von GFI EndPointSecurity**.

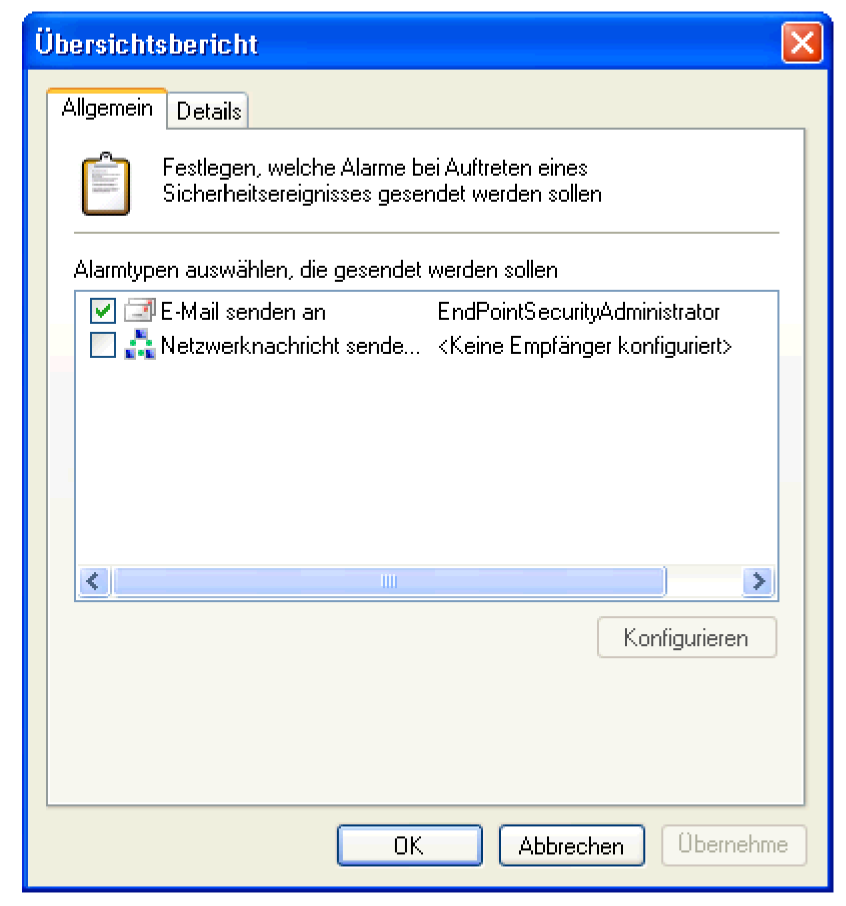
So konfigurieren Sie den Übersichtsbericht:

1. Klicken Sie in der GFI EndPointSecurity-Verwaltungskonsole auf die Registerkarte **Konfiguration**.

2. Klicken Sie auf die untergeordnete Registerkarte **Optionen**.

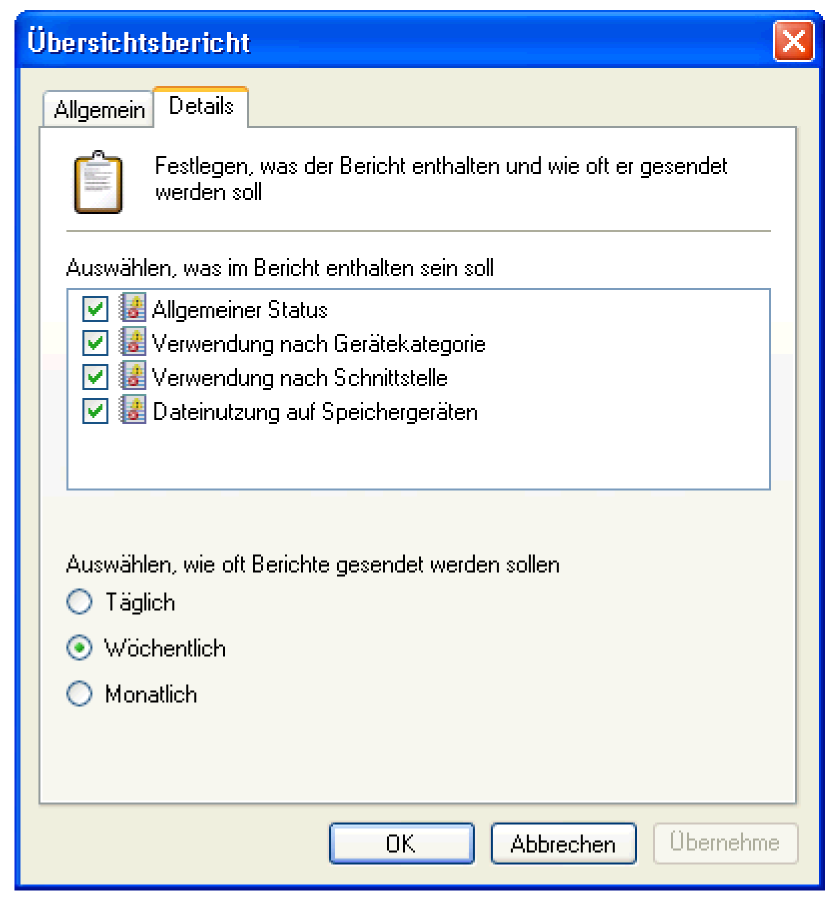
3. Klicken Sie auf den Knoten **Warnoptionen**.

4. Klicken Sie im rechten Bereich unter **Warnoptionen** auf den Hyperlink **Übersichtsbericht konfigurieren**.




*Screenshot 112 - Optionen für Übersichtsbericht - Reiter „Allgemein“*

5. Wählen Sie im Dialog **Übersichtsbericht** die Registerkarte **Allgemein**.
6. Aktivieren bzw. deaktivieren Sie die zu sendenden Warnmeldungen.
7. Markieren Sie eine aktivierte Warnmeldung, und klicken Sie auf **Konfigurieren**, um Benutzer/Gruppen als Empfänger anzugeben.




*Screenshot 113 - Optionen für Übersichtsbericht - Reiter „Details“*

8. Wählen Sie die Registerkarte **Details**, um den Inhalt des Berichts festzulegen, der von GFI EndPointSecurity gesendet wird.

9. Aktivieren bzw. deaktivieren Sie die Elemente, die im Bericht enthalten sein sollen:

   » Allgemeiner Status

   » Gerätenutzung nach Gerätetyp

   » Gerätenutzung nach Schnittstellen

   » Dateinutzung auf Speichergeräten

10. Legen Sie die Häufigkeit der Berichte fest, indem Sie **Täglich**, **Wöchentlich** oder **Monatlich** auswählen, und klicken Sie auf **OK**.

## 10.8 Konfigurieren des Datenbank-Backends

GFI EndPointSecurity ermöglicht die Nachverfolgung aller Ereignisse, die durch GFI EndPointSecurity-Agenten auf kontrollierten Computern verursacht werden.

Nach der Installation von GFI EndPointSecurity haben Sie folgende Möglichkeiten:

» Laden Sie Microsoft SQL Server Express Edition herunter und installieren Sie es, um automatisch eine Datenbank für GFI EndPointSecurity zu erstellen. Dies kann über den Schnellstart-Assistenten erfolgen.

» Stellen Sie eine Verbindung mit einem vorhandenen Microsoft SQL Server her, und Sie können entweder eine vorhandene Datenbank verwenden oder eine neue erstellen. Dies kann über den Schnellstart-Assistenten oder die untergeordneten Registerkarten „Allgemeiner Status“ oder „Optionen“ erfolgen.

In diesem Abschnitt erfahren Sie, wie Sie über die untergeordneten Registerkarten „Allgemeiner Status“ und „Optionen“ eine Verbindung mit einem verfügbaren Microsoft SQL Server herstellen können.

Weitere Informationen zum Herunterladen und Installieren von Microsoft SQL Server Express Edition oder zum Herstellen einer Verbindung mit einem verfügbaren Microsoft SQL Server über den Schnellstart-Assistenten finden Sie in „GFI EndPointSecurity – Erste Schritte“.

### 10.8.1 Herstellen einer Verbindung mit einem verfügbaren SQL Server

So greifen Sie auf die Einstellungen des Datenbank-Backends zu:

Option 1: Zugriff über die Registerkarte „Allgemein“:

1. Klicken Sie in der GFI EndPointSecurity-Verwaltungskonsole auf die Registerkarte **Status**.

2. Klicken Sie auf die untergeordnete Registerkarte **Allgemein**.

3. Klicken Sie unter **Status des Datenbank-Backends** auf den Hyperlink **Datenbank konfigurieren...**.

Option 2: Zugriff über die Registerkarte „Optionen“:

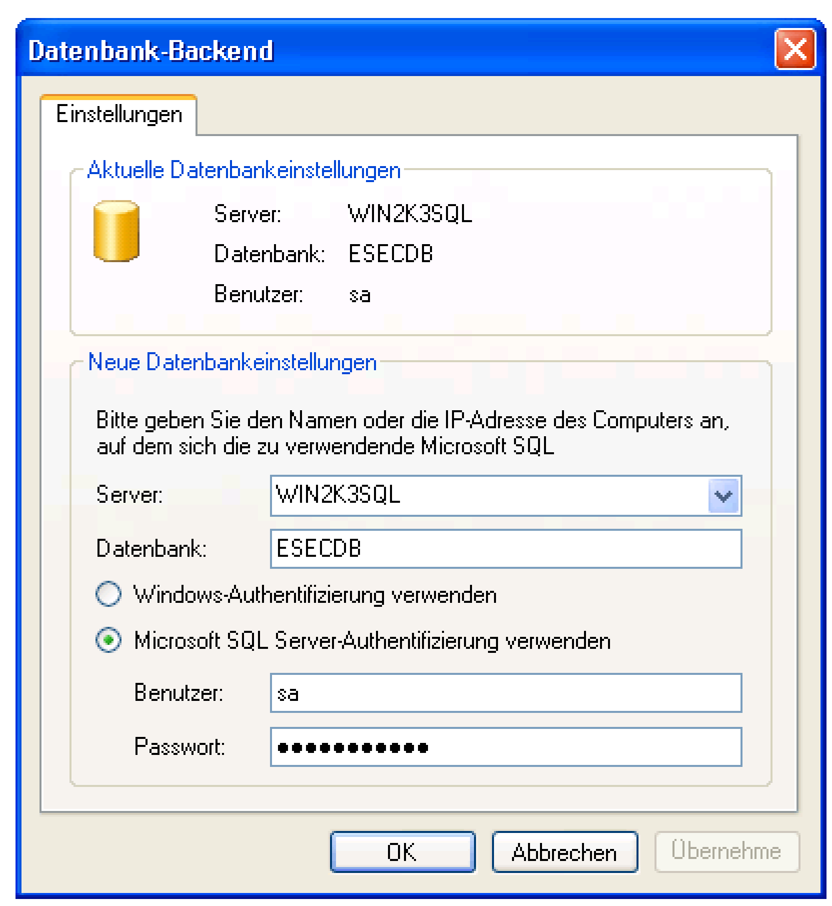
1. Klicken Sie in der GFI EndPointSecurity-Verwaltungskonsole auf die Registerkarte **Konfiguration**.

2. Klicken Sie auf die untergeordnete Registerkarte **Optionen**.

3. Klicken Sie auf den Knoten **Datenbank-Backend**.

4. Klicken Sie im rechten Bereich unter **Datenbank-Backend** auf den Hyperlink **Datenbank-Backend ändern**.

So stellen Sie eine Verbindung mit einem verfügbaren SQL Server her und erstellen entweder ein neues Datenbank-Backend oder ändern die Einstellungen für das Datenbank-Backend:




*Screenshot 114 - Optionen für Datenbank-Backend*

1. Geben Sie im Dialog **Datenbank-Backend** den Servernamen/die IP-Adresse eines verfügbaren Datenbankservers ein. Oder wählen Sie eine neue SQL-Installation aus dem Dropdown-Menü **Server** aus.

2. Geben Sie in das Feld **Datenbank** den Namen der Datenbank ein.

3. Wählen Sie für die Verbindung mit dem Server des Datenbank-Backends die gewünschte Authentifizierungsmethode aus, und klicken Sie auf **OK**.



Bei der Auswahl von **Microsoft SQL Server-Authentifizierung verwenden** muss ein Benutzername und ein Kennwort für den Server des Datenbank-Backends eingegeben werden.

### 10.8.2 Warten des Datenbank-Backends

Die Datenbank muss regelmäßig gewartet werden, um weiterhin effizient nutzbar zu sein. Es stehen mehrere Parameter zur Verfügung, mit denen sich die automatische Wartung des Datenbank-Backends steuern lässt.

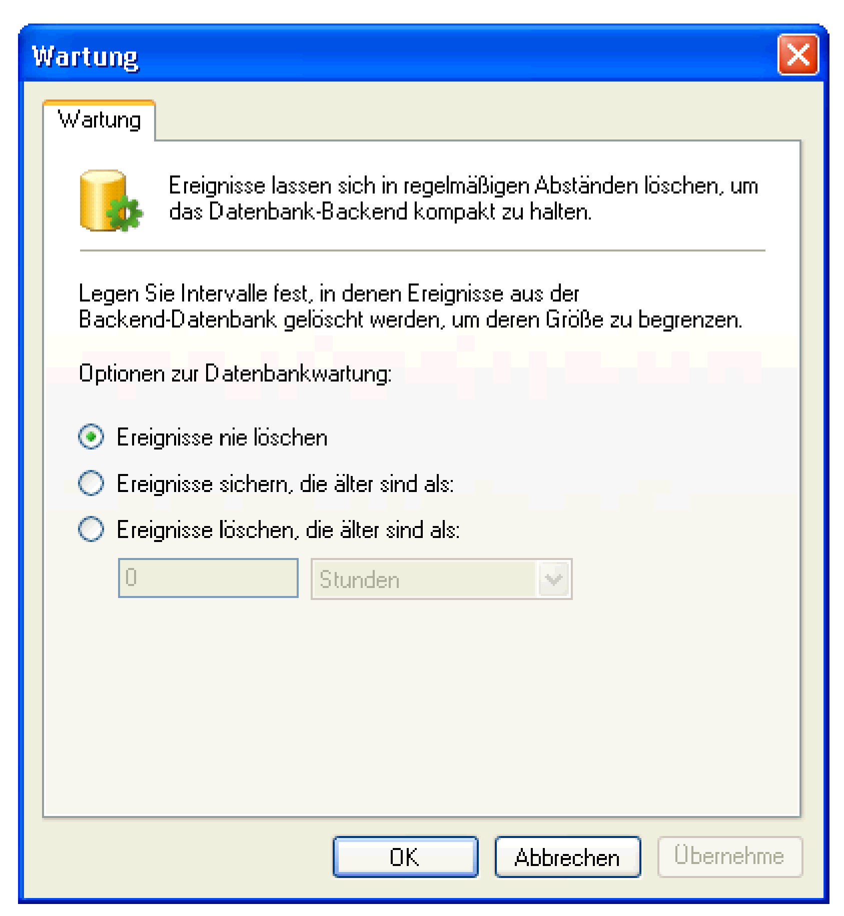
So konfigurieren Sie die Wartung des Datenbank-Backends:

1. Klicken Sie in der GFI EndPointSecurity-Verwaltungskonsole auf die Registerkarte **Konfiguration**.

2. Klicken Sie auf die untergeordnete Registerkarte **Optionen**.

3. Klicken Sie auf den Knoten **Datenbank-Backend**.

4. Klicken Sie im rechten Bereich unter **Datenbank-Backend** auf den Hyperlink **Datenbankwartung**.




*Screenshot 115 - Wartungsoptionen*

5. Wählen Sie im Dialog **Wartung** die erforderliche Option für die Datenbankwartung aus:

- Ereignisse nie löschen
- **Ereignisse sichern, die älter sind als** – Geben Sie im dafür vorgesehen Feld und Dropdown-Menü das Zeitintervall in Stunden/Tagen an, in dem Ereignisse gesichert werden sollen. Mit dieser Option werden Ereignisse automatisch vom Datenbank-

Backend in die Sicherungsdatenbank verschoben, sobald ein Ereignis gesichert wurde.

» **Ereignisse löschen, die älter sind als** – Geben Sie im dafür vorgesehen Feld und Dropdown-Menü das Zeitintervall in Stunden/Tagen an, in dem Ereignisse aus dem Datenbank-Backend gelöscht werden sollen. Gelöschte Datenbankeinträge können nicht wiederhergestellt werden.

6. Klicken Sie auf **OK**.

## 10.9 Konfigurieren von Benutzermeldungen

GFI EndPointSecurity ermöglicht das Anpassen der Meldungen, die von GFI EndPointSecurity-Agenten auf Zielcomputern angezeigt werden, wenn auf ein Gerät zugegriffen wird.

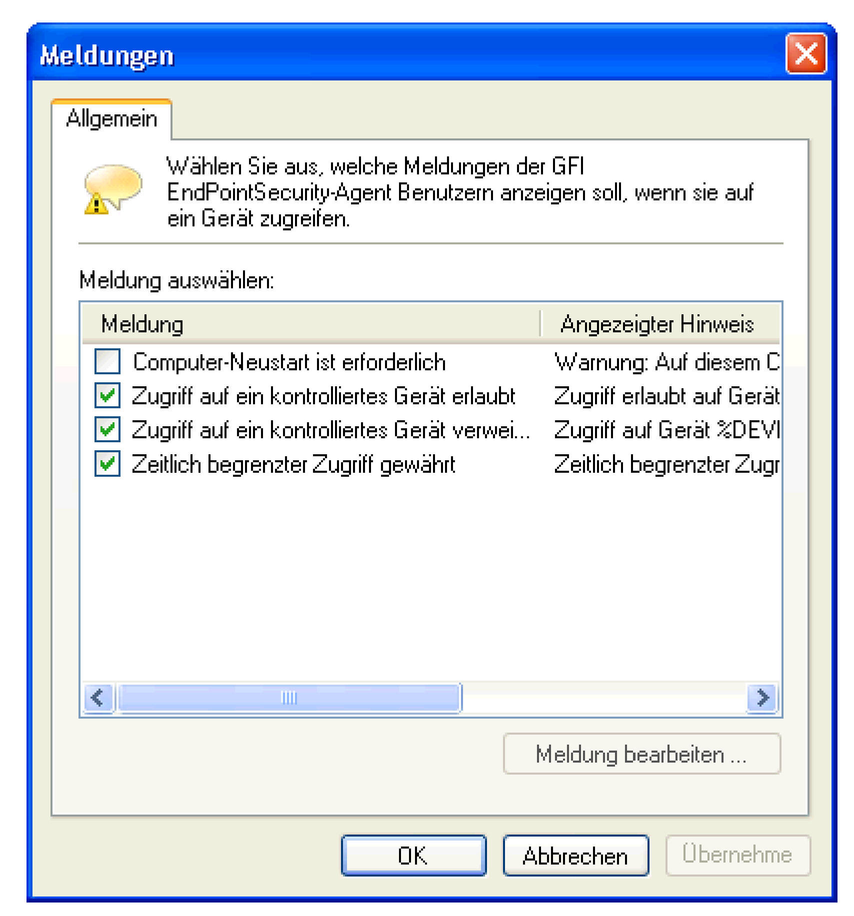
So passen Sie diese Meldungen zum Gerätezugriff an:

1. Klicken Sie in der GFI EndPointSecurity-Verwaltungskonsole auf die Registerkarte **Konfiguration**.

2. Klicken Sie auf die untergeordnete Registerkarte **Optionen**.

3. Klicken Sie auf den Knoten **Anpassbare Popup-Meldungen**.

4. Klicken Sie im rechten Bereich unter **Anpassbare Popup-Meldungen** auf den Hyperlink **Meldungen anpassen**.




*Screenshot 116 - Optionen für anpassbare Popup-Meldungen*

5. Aktivieren bzw. deaktivieren Sie im Dialog **Anpassbare Popup-Meldungen** die gewünschten Meldungen.

6. Markieren Sie eine aktivierte Meldung, und klicken Sie auf **Meldung bearbeiten…**, um sie nach Bedarf zu ändern. Klicken Sie anschließend auf **Speichern**.

Wiederholen Sie diesen Schritt für jede Meldung, die Sie bearbeiten möchten.

7. Klicken Sie auf **OK**.

## 10.10 Konfigurieren von erweiterten GFI EndPointSecurity-Optionen

GFI EndPointSecurity ermöglicht das Konfigurieren der folgenden Einstellungen von GFI EndPointSecurity-Agenten:

- TCP/IP-Port für die Hauptkommunikation
- Bereitstellungsoptionen
- Passwort zur Agentenkontrolle

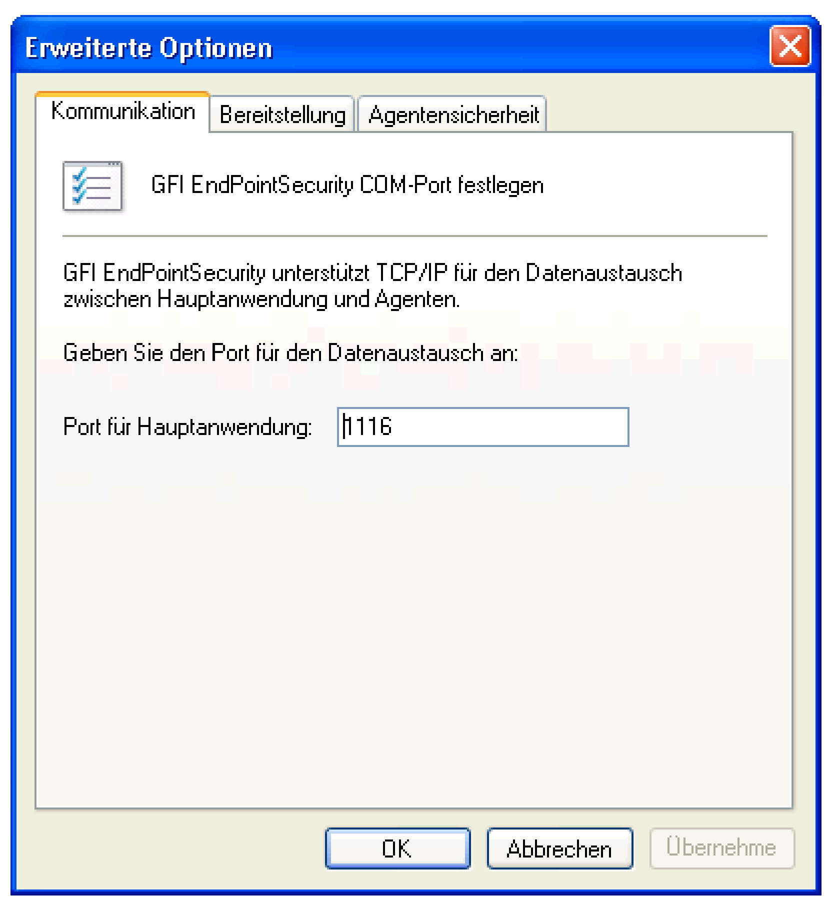
So konfigurieren Sie die erweiterten Optionen:

1. Klicken Sie in der GFI EndPointSecurity-Verwaltungskonsole auf die Registerkarte **Konfiguration**.

2. Klicken Sie auf die untergeordnete Registerkarte **Optionen**.

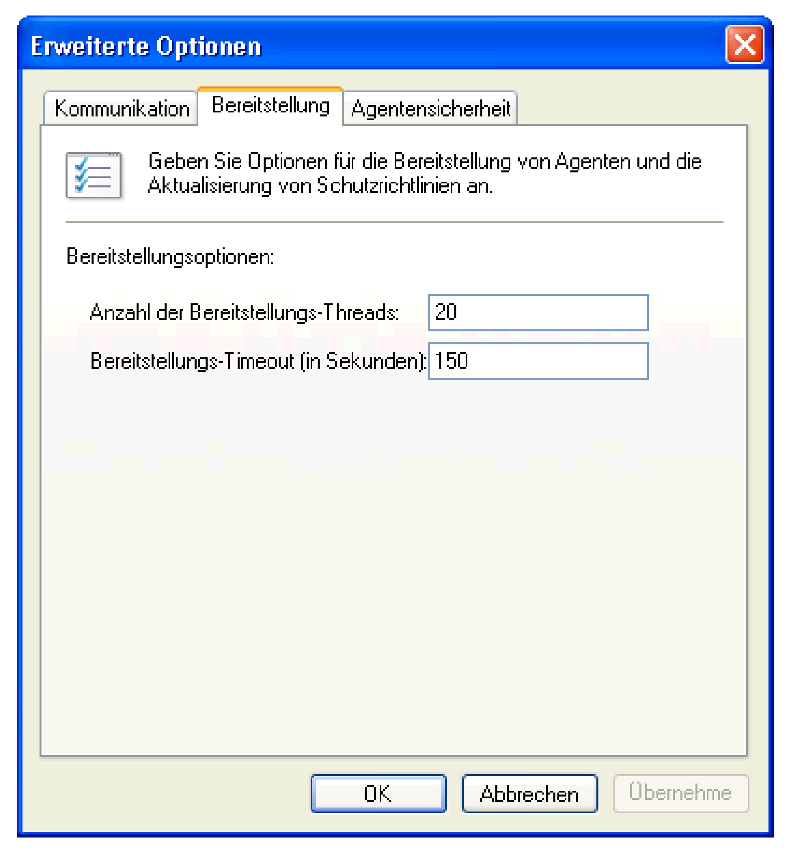
3. Klicken Sie auf den Knoten **Erweiterte Optionen**.

4. Klicken Sie im rechten Bereich unter **Erweiterte Optionen** auf den Hyperlink **Erweiterte Optionen bearbeiten**.



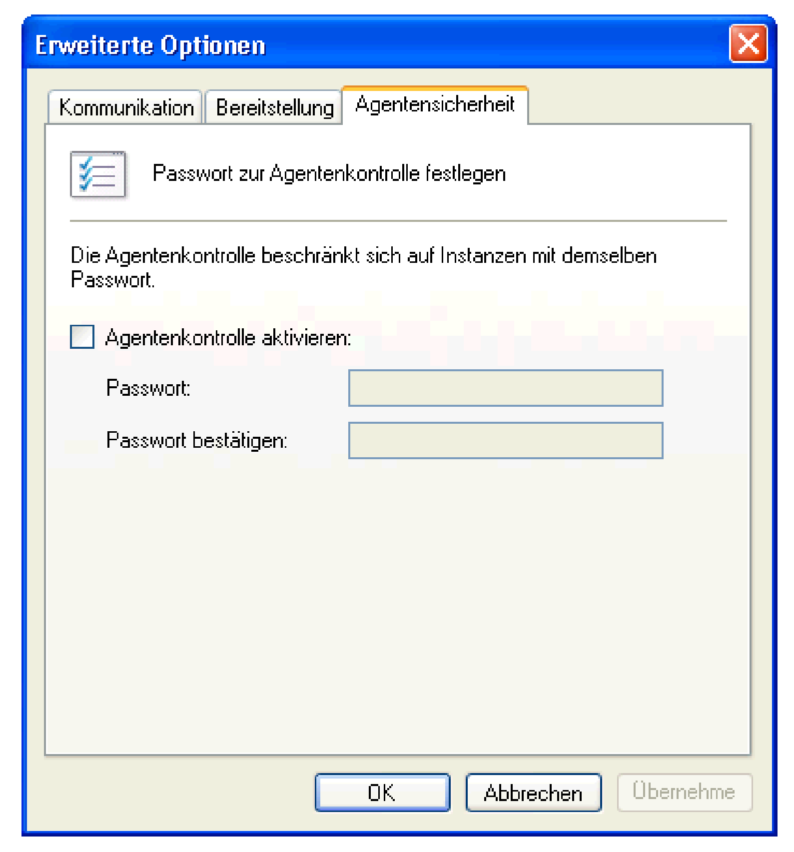

*Screenshot 117 - Erweiterte Optionen - Registerkarte „Kommunikation“*

5. Wählen Sie im Dialog **Erweiterte Optionen** die Registerkarte **Kommunikation**, und geben Sie die für die Kommunikation zwischen der GFI EndPointSecurity-Verwaltungskonsole und den GFI EndPointSecurity-Agenten erforderliche TCP/IP-Portnummer ein (TCP/IP 1116 ist die Standard-Portnummer).




*Screenshot 118 - Erweiterte Optionen - Registerkarte „Bereitstellung"*

6. Wählen Sie die Registerkarte **Bereitstellung**, und geben Sie unter **Anzahl der Bereitstellungs-Threads** und **Bereitstellungs-Timeout (in Sekunden)** die erforderlichen Werte ein.




*Screenshot 119 - Erweiterte Optionen - Registerkarte „Agentensicherheit"*

7. Wählen Sie die Registerkarte **Agentensicherheit**, und aktivieren bzw. deaktivieren Sie die Option **Agentenkontrolle aktivieren**. Geben Sie bei aktivierter Option das Agentenpasswort ein.



Der Schutz kann nur für Agenten bereitgestellt werden, die das festgelegte Kennwort verwenden.

8. Klicken Sie auf **OK**.

# 11 Deinstallation von GFI EndPointSecurity

## 11.1 Einführung

GFI EndPointSecurity ermöglicht die Deinstallation von GFI EndPointSecurity-Agenten und der GFI EndPointSecurity-Anwendung.

In diesem Kapitel werden folgenden Themen behandelt:

» Deinstallation von GFI EndPointSecurity-Agenten

» Deinstallation der GFI EndPointSecurity-Anwendung



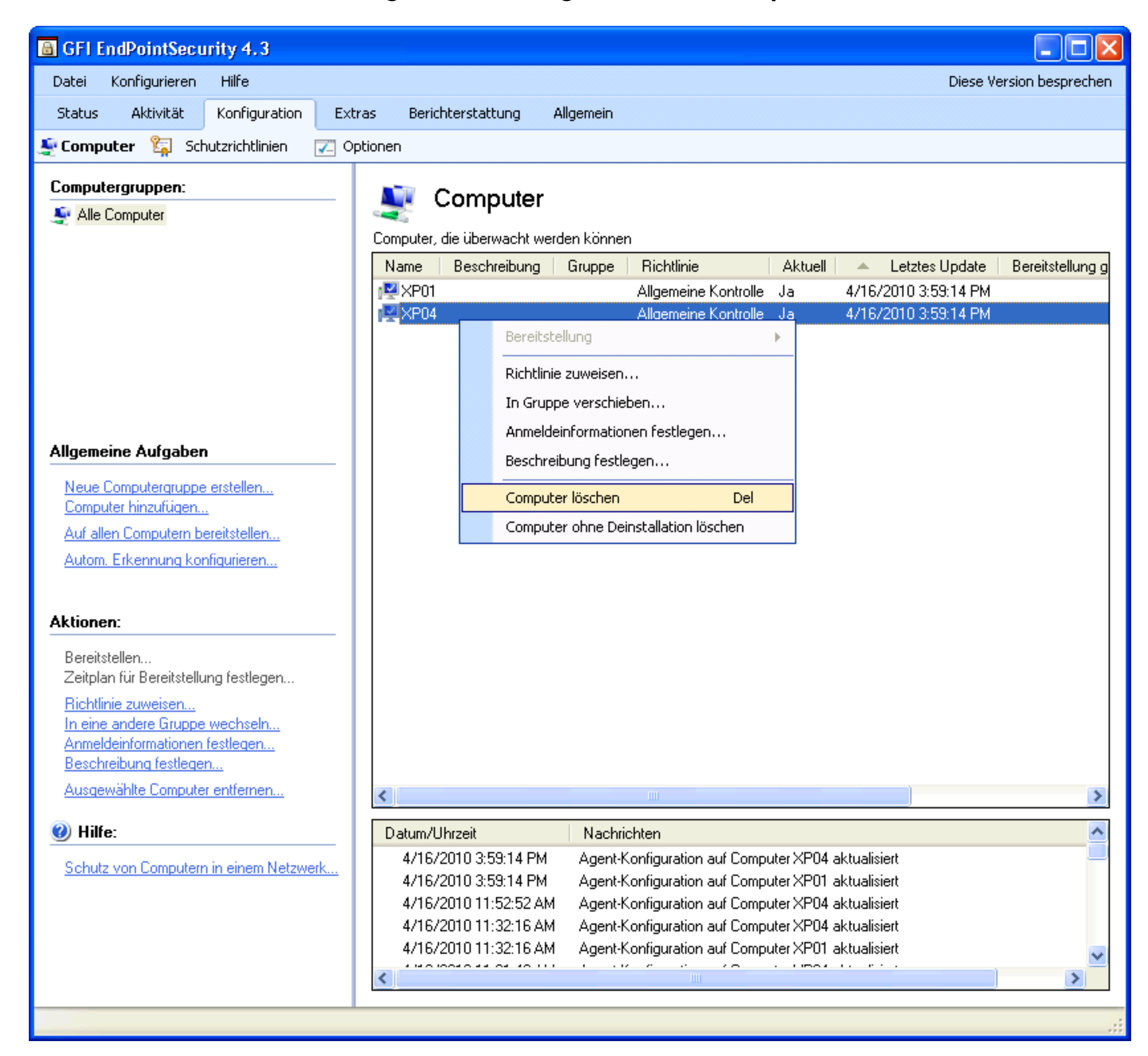
**GFI EndPointSecurity-Agenten werden bei der Deinstallation der GFI EndPointSecurity-Anwendung nicht automatisch deinstalliert. Deinstallieren Sie zunächst die GFI EndPointSecurity-Agenten, bevor Sie die GFI EndPointSecurity-Anwendung deinstallieren.**

## 11.2 Deinstallation von GFI EndPointSecurity-Agenten

So deinstallieren Sie einen GFI EndPointSecurity-Agenten:

1. Klicken Sie in der GFI EndPointSecurity-Verwaltungskonsole auf die Registerkarte **Konfiguration**.

2. Klicken Sie auf die untergeordnete Registerkarte **Computer**.



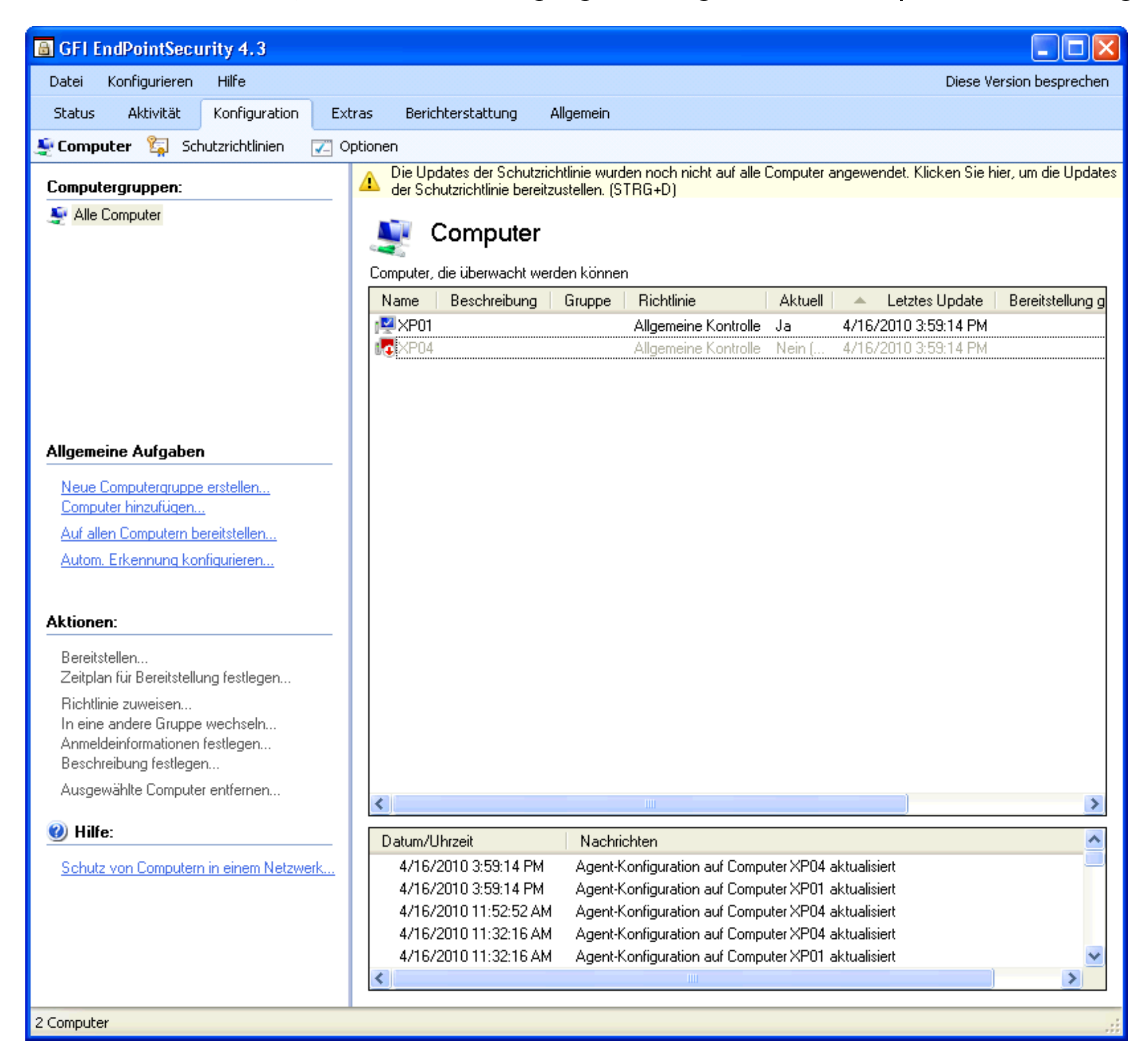

*Screenshot 120 - untergeordnete Registerkarte „Computer“ - Computer löschen*

3. Klicken Sie im rechten Fenster mit der rechten Maustaste auf den Zielcomputer, den sie löschen möchten. Folgende Optionen stehen im Kontextmenü zur Verfügung:

» **Computer löschen** - Der GFI EndPointSecurity-Agent wird vom Zielcomputer deinstalliert, nachdem die Updates der Schutzrichtlinie bereitgestellt wurden.

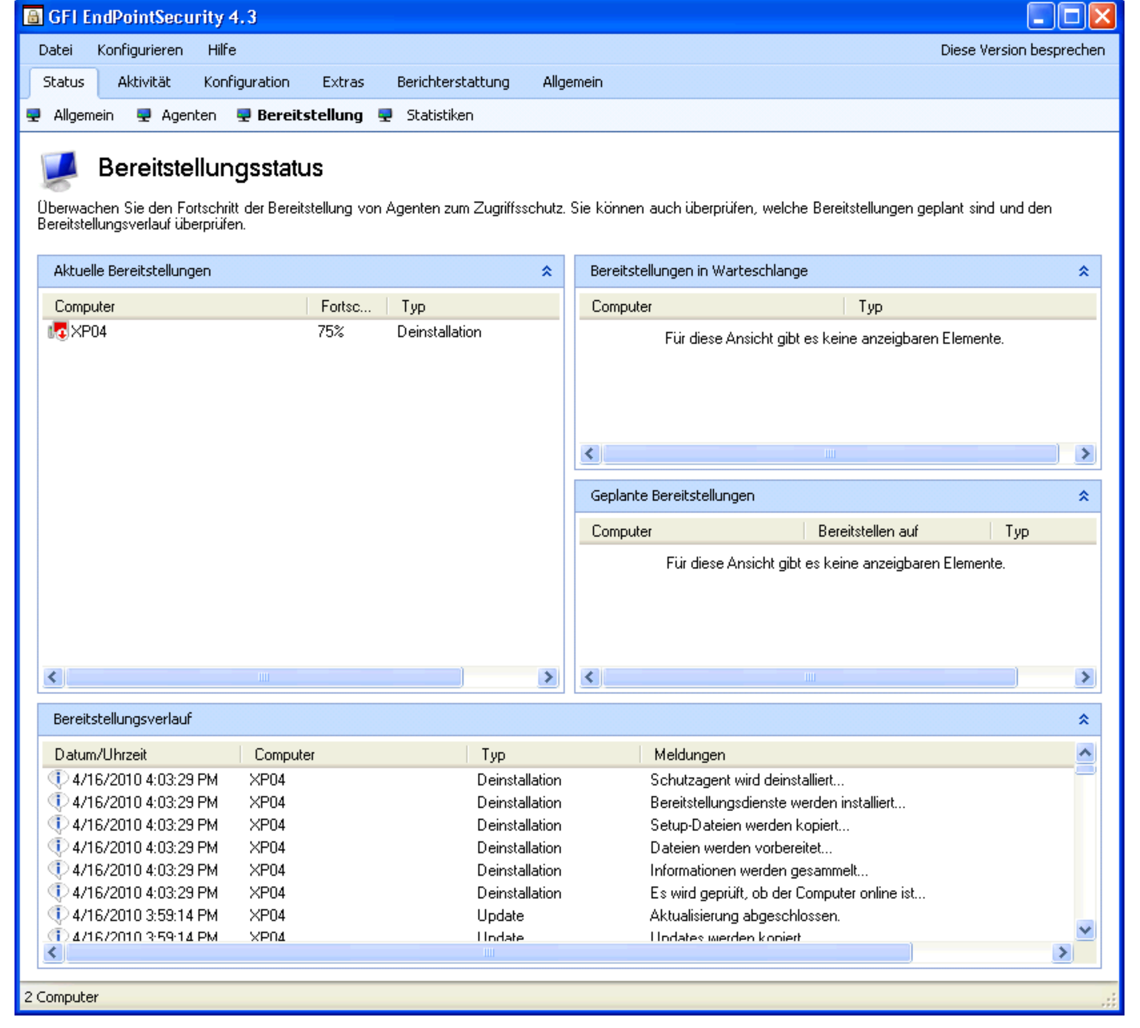
» **Computer ohne Deinstallation löschen** – Der entsprechende Computereintrag wird aus der Liste Computer entfernt, aber der Agent bleibt weiterhin auf dem Zielcomputer installiert. Diese Option ist geeignet, wenn der Zielcomputer aus dem Netzwerk entfernt wurde und die GFI EndPointSecurity-Anwendung keine Verbindung zu diesem Computer herstellen kann, um den Agenten zu deinstallieren.

4. Klicken Sie auf **Ja**, um den Löschvorgang des ausgewählten Computers zu bestätigen.




*Screenshot 121 - untergeordnete Registerkarte „Computer“ - noch offene Deinstallation*

5. Klicken Sie im rechten Bereich auf die oberste Warnmeldung, um die Updates für Schutzrichtlinien bereitzustellen. Die Ansicht sollte automatisch zu **Status** ► **Bereitstellung** wechseln.




*Screenshot 122 - untergeordnete Registerkarte „Bereitstellung“*

6. Prüfen Sie im Bereich **Bereitstellungsverlauf** den erfolgreichen Abschluss der Deinstallation vom Zielcomputer.

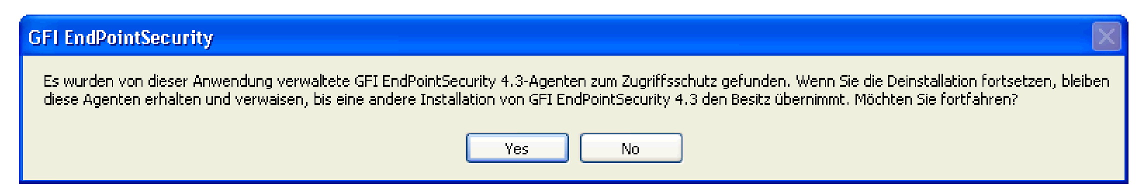
## 11.3 Deinstallation der GFI EndPointSecurity-Anwendung

So deinstallieren Sie die GFI EndPointSecurity-Anwendung:



Führen Sie das Deinstallationsprogramm als Administrator auf dem Computer aus.

1. Wählen Sie in der **Microsoft Windows-Systemsteuerung** die Optionen **Software** bzw. **Programme und Funktionen**.
2. Wählen Sie **GFI EndPointSecurity**.
3. Klicken Sie auf **Ändern**, um die Deinstallation der GFI EndPointSecurity-Anwendung zu starten.
4. Klicken Sie auf dem Willkommensbildschirm auf **Weiter**, um mit der Deinstallation fortzufahren.




*Screenshot 123 - Informationsmeldung zur Deinstallation*



Wenn Agenten noch auf dem Computer installiert sind, werden Sie in einem Informationsdialog gefragt, ob Sie mit der Deinstallation fortfahren möchten (die Agenten bleiben auf dem Computer installiert und als verwaiste Agenten erhalten), oder ob Sie die Deinstallation abbrechen möchten. Weitere Informationen zur Deinstallation von Agenten finden Sie im Abschnitt **Deinstallation von GFI EndPointSecurity-Agenten** in diesem Kapitel.

5. Wählen Sie die Option **Deinstallieren, aber Konfigurationsdateien beibehalten** oder **Vollständig deinstallieren**, und klicken Sie zum Fortfahren auf **Weiter**.
6. Klicken Sie nach Abschluss der Deinstallation auf **Fertig stellen**.

# 12 Diverses

## 12.1 Einführung

Dieses Kapitel beinhaltet alle Informationen, die nicht der Erstkonfiguration von GFI EndPointSecurity zugeordnet werden können.

## 12.2 Eingeben des Lizenzschlüssels nach der Installation

Nach der Installation von GFI EndPointSecurity können Sie den Lizenzschlüssel eingeben, ohne die Anwendung erneut zu installieren oder zu konfigurieren.

So geben Sie Ihren Lizenzschlüssel ein:

1. Klicken Sie in der GFI EndPointSecurity-Verwaltungskonsole auf die Registerkarte **Allgemein**.

2. Wählen Sie im linken Bereich die Option **Lizenzierung**.

3. Klicken Sie im rechten Bereich unter **Lizenzierung** auf den Hyperlink **(Bearbeiten...)**.




*Screenshot 124 - Bearbeitung des Lizenzschlüssels*

4. Geben Sie im Textfeld **Lizenzschlüssel** den Lizenzschlüssel ein, den Sie von GFI Software Ltd. erhalten haben.

5. Klicken Sie auf **OK**, um den Lizenzschlüssel zu übernehmen.

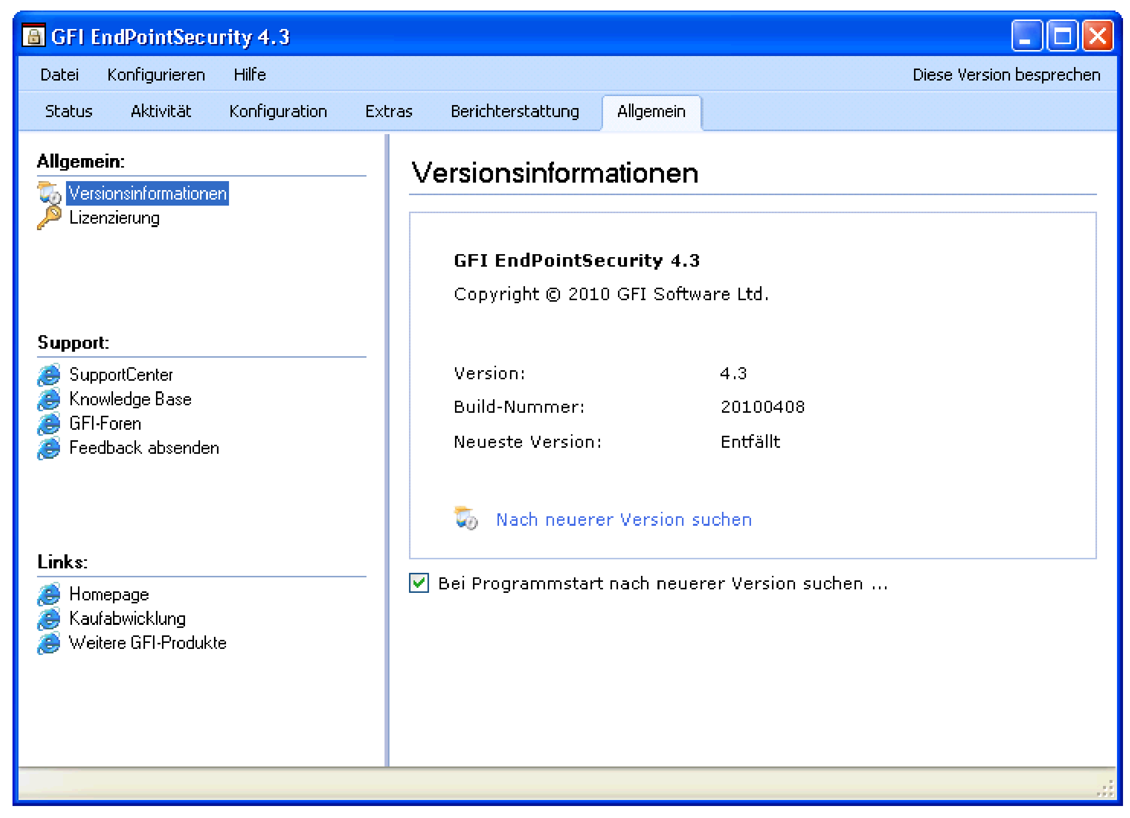
## 12.3 Prüfen auf neuere Versionen von GFI EndPointSecurity

GFI Software veröffentlicht regelmäßig Produkt-Updates, die manuell oder automatisch von der GFI-Website heruntergeladen werden können.

So prüfen Sie, ob eine neuere Version von GFI EndPointSecurity zum Herunterladen verfügbar ist:

1. Klicken Sie in der GFI EndPointSecurity-Verwaltungskonsole auf die Registerkarte **Allgemein**.

2. Klicken Sie im linken Navigationsbereich auf **Versionsinformationen**.




*Screenshot 125 - Registerkarte „Allgemeint“ - Bereich „Versionsinformationen“*

3. Klicken Sie im rechten Bereich auf den Hyperlink **Auf neuere Version prüfen**, um zu überprüfen, ob eine neuere Version von GFI EndPointSecurity zur Verfügung steht. Aktivieren Sie alternativ das Kontrollkästchen **Beim Start auf neuere Version prüfen**, um bei jedem Start von GFI EndPointSecurity automatisch zu prüfen, ob eine neuere Version zum Herunterladen verfügbar ist.

# 13 Fehlerbehebung

## 13.1 Einführung

In diesem Kapitel werden Vorgehensweisen zur Behebung möglicher Softwareprobleme erläutert. Die wichtigsten Informationsquellen für Benutzer sind die folgenden:

- Das Handbuch – die meisten Probleme lassen sich mit Hilfe dieses Handbuchs lösen
- Artikel aus der GFI Knowledge Base
- Webforum
- Der technische Support von GFI Software

## 13.2 Häufige Probleme

| Aufgetretenes Problem | Lösung |
| --- | --- |
| Im Bereich **Status ► Bereitstellung ► Bereitstellungsverlauf** werden nach der Bereitstellung von GFI EndPointSecurity-Agenten durch die GFI EndPointSecurity-Verwaltungskonsole Fehler angezeigt. | Weitere Informationen zu Fehlermeldungen, deren Ursachen und mögliche Lösungen finden Sie im **Anhang 1 - Bereitstellungsfehlermeldungen** dieses Handbuchs. |

## 13.3 Knowledge Base

GFI pflegt eine Knowledge Base, in der Lösungen für die häufigsten Probleme beschrieben sind. Informieren Sie sich bei einem Problem zuerst immer in der Knowledge Base. Die Knowledge Base enthält immer die aktuelle Liste der Fragen, die an den technischen Support gerichtet wurden, sowie die neuesten Patches. Unter **http://kbase.gfi.com/** können Sie auf die Knowledge Base zugreifen.

## 13.4 Webforum

Über das Webforum erhalten Sie technischen Support von Benutzer zu Benutzer. Das Forum finden Sie unter: **http://forums.gfi.com/**.

## 13.5 Technischen Support anfragen

Falls Sie ein Softwareproblem mit Hilfe dieses Handbuchs und der Artikel in der Knowledge Base nicht lösen konnten, wenden Sie sich online über eine Support-Anfrage oder per Telefon an das Team des Technischen Supports von GFI.

- Online: Bitte füllen Sie unser Online-Support-Formular aus: **http://support.gfi.com/supportrequestform.asp**.
- Telefon: Auf der folgenden Seite erhalten Sie die landesspezifische Telefonnummer für den technischen Support: **http://www.gfi.com/company/contact.htm**.



Halten Sie Ihre Kundennummer bereit, wenn Sie sich an den technischen Support wenden. Ihre Kundennummer entspricht der Online-Kontonummer, die Sie bei der ersten Registrierung Ihrer Lizenzschlüssel im Kundenbereich unter folgendem Link erhalten haben: **http://customers.gfi.com**.

Für die Beantwortung Ihrer Anfrage benötigt GFI in Abhängigkeit von Ihrer Zeitzone maximal 24 Stunden.

## 13.6 Build-Benachrichtigungen

Benutzern wird ausdrücklich empfohlen, die Mailingliste für Build-Benachrichtigungen zu abonnieren. Auf diese Weise werden Sie sofort über neue Produkt-Builds informiert. Rufen Sie hierzu den folgenden Link auf: **http://www.gfi.com/pages/productmailing.htm**.

## 13.7 Dokumentation

Wenn dieses Handbuch Ihre Erwartungen nicht erfüllt, oder wenn Sie denken, dass diese Dokumentation auf irgendeine Weise verbessert werden kann, zögern Sie nicht, uns per E-Mail Ihre Meinung mitzuteilen: **documentation@gfi.com**.

# 14 Glossar

| | |
|---|---|
| **Active Directory** | Eine Technologie, die verschiedene Netzwerkdienste bereitstellt (inkl. LDAP-artige Verzeichnisdienste). |
| **Administratorkonto für Alarme** | Ein Alarmempfängerkonto, das automatisch nach der Installation von GFI EndPointSecurity erstellt wird. |
| **Alarme** | Benachrichtigungen (E-Mail-Warnungen, Netzwerknachrichten oder SMS-Nachrichten), die beim Auftreten eines bestimmten Ereignisses an Alarmempfänger gesendet werden. |
| **Alarmempfänger** | Ein GFI EndPointSecurity-Profilkonto, das die Kontaktdetails von Benutzern enthält, die E-Mail-Warnungen und Netzwerk- bzw. SMS-Nachrichten erhalten sollen. |
| **Assistent zur Erstellung von Schutzrichtlinien** | Ein Assistent für die Erstellung und Konfiguration von neuen Schutzrichtlinien. Konfigurationseinstellungen beinhalten die Auswahl von zu kontrollierenden Gerätekategorien und Schnittstellen sowie die Festlegung, ob diese zugängig oder blockiert sind. Dieser Assistent ermöglicht außerdem die Konfiguration von Dateitypfiltern, von Verschlüsselungsberechtigungen sowie von Protokollierungs- und Warnoptionen. |
| **Automatische Suche** | Eine zeitgesteuerte GFI EndPointSecurity-Funktion zur Suche und Erkennung von Computern, die neu im Netzwerk angeschlossen wurden. |
| **Benutzerbenachrichtigung** | Eine Nachricht, die von GFI EndPointSecurity-Agenten auf kontrollierten Computer angezeigt wird, wenn ein Zugriff auf Geräte erfolgt. |
| **Bereitstellungsfehlermeldungen** | Fehler, die nach der Bereitstellung der GFI EndPointSecurity-Agenten durch die GFI EndPointSecurity-Verwaltungskonsole auftreten können. |
| **BitLocker To Go** | Eine Funktion von Microsoft Windows 7, zum Schutz und zur Verschlüsselung von Daten auf Wechseldatenträgern. |
| **Dateityp-Filter** | Ein Satz von Einschränkungen, die Benutzer und Gruppen auf Dateitypbasis zugewiesen werden. Die Filterung basiert auf der Überprüfung von Dateierweiterungen und Echtzeitüberprüfungen des wahren Dateityps. |
| **Datenbank-Backend** | Eine von GFI EndPointSecurity genutzte Datenbank, in der alle von GFI EndPointSecurity-Agenten auf kontrollierten Computern erzeugten Ereignisse in der Form eines Audit-Trails gespeichert werden. |
| **Eingabegeräte** | Eine Spezifikation, die Teil des Universal Serial Bus (USB)-Standards für eine Klasse von Peripheriegeräten ist. Diese Geräte, wie Mäuse, Tastaturen und Joysticks, ermöglichen dem Benutzer die Eingabe von Daten oder die direkte Interaktion mit dem Computer. |
| **Ereignisprotokollierung** | Eine GFI EndPointSecurity-Funktion, die auf kontrollierten Computern alle Ereignisse zu Zugriffsversuchen auf Geräte und Schnittstellen erfasst. |
| **Geräte-Blacklist** | Eine Liste einzelner Geräte, deren Zugriff auf Computern blockiert wird, die der Schutzrichtlinie angehören. |
| **Gerätekategorie** | Eine Gruppe von Peripheriegeräten, die in einer Kategorie verwaltet werden. |
| **Geräte-Scan** | Eine GFI EndPointSecurity-Funktion, zur Suche aller Geräte, die an kontrollierten Computern angeschlossen sind und waren. |
| **Geräte-Whitelist** | Eine Liste einzelner Geräte, deren Zugriff auf Computern zugelassen wird, die der Schutzrichtlinie angehören. |
| **GFI EndPointSecurity-Agent** | Ein Agent auf den zu kontrollierenden Computern, der dafür sorgt, dass die Schutzrichtlinien auf diesen Computern eingerichtet und durchgesetzt werden. |
| **GFI EndPointSecurity-Anwendung** | Eine Sicherheitsanwendung auf dem Server, die die Integrität von Daten sichert und den unautorisierten Zugriff auf tragbare Speichermedien sowie den Datenaustausch auf und von Hardware und Schnittstellen verhindert. |
| **GFI EndPointSecurity-Verwaltungskonsole** | Die Benutzeroberfläche von GFI EndPointSecurity auf dem Server. |

| | |
|---|---|
| **Globale Berechtigungen** | Ein Schritt innerhalb des Assistenten zur Erstellung von Schutzrichtlinien, der den Benutzer auffordert, den Zugriff auf alle Geräte zu gewähren oder zu blockieren, die einer Kategorie angehören oder die an eine Schnittstelle eines Computers angeschlossen sind, der durch die Schutzrichtlinie kontrolliert wird. |
| **GPO (Group Policy Object)** | *Siehe* Gruppenrichtlinienobjekte. |
| **Gruppenrichtlinienobjekte** | Ein zentralisiertes Active Directory-Verwaltungs- und Konfigurationssystem, das festlegt, was Benutzern in einem Computernetzwerk erlaubt und untersagt ist. |
| **Hauptbenutzer** | Ein Hauptbenutzer besitzt automatisch vollen Zugriff auf alle Geräte, die am von der Schutzrichtlinie kontrollierten Computer angeschlossen sind. |
| **Kontrollierter Computer** | Ein Computer, der durch eine GFI EndPointSecurity-Schutzrichtlinie geschützt wird. |
| **MSI-Datei** | Eine von GFI EndPointSecurity generierte Datei für die spätere Bereitstellung mithilfe von Gruppenrichtlinienobjekten oder anderen Bereitstellungsoptionen. Diese Datei kann für alle Schutzrichtlinien generiert werden und enthält alle konfigurierten Sicherheitseinstellungen. Dazu gehören auch Installationseinstellungen für ungeschützte Computer. |
| **Schnellstart-Assistent** | Ein Assistent für die benutzerdefinierte Konfiguration von GFI EndPointSecurity. Er wird beim ersten Start der GFI EndPointSecurity-Verwaltungskonsole automatisch gestartet. |
| **Schnittstelle** | Eine physische Verbindungsstelle zwischen Computern und Geräten. |
| **Schutzrichtlinie** | Ein Berechtigungssatz für den Zugriff auf Geräte und Schnittstellen, der unternehmensspezifisch konfiguriert werden kann. |
| **Sicherheitsverschlüsselung** | Ein Einschränkungssatz, der Benutzern/Gruppen den Zugriff auf Dateitypen gewährt oder blockiert, die mit BitLocker To Go verschlüsselt auf Geräten gespeichert sind. Diese Einschränkungen werden angewendet, wenn verschlüsselte Geräte an die durch die Schutzrichtlinie kontrollierten Computer angeschlossen werden. |
| **Temporary-Access-Tool von GFI EndPointSecurity** | Ein Tool auf kontrollierten Computern. Es wird vom Benutzer dafür verwendet, einen Anfragecode zu generieren und später einen Entsperrcode einzugeben, um einen zeitlich begrenzten Zugriff zu aktivieren, sobald dieser vom Administrator gewährt wird.<br>Bei Aktivierung hat der Benutzer auf seinem kontrollierten Computer für eine bestimmte Dauer und ein bestimmtes Zeitfenster Zugriff auf Geräte und Schnittstellen (wenn der Zugriff normalerweise blockiert wird). |
| **Übersichtsbericht** | Eine zusammenfassender Bericht mit statistischen Daten zur von GFI EndPointSecurity erfassten Kontoaktivität. |
| **Zugriffsberechtigungen** | Berechtigungen (Zugriff, Lesen und Schreiben), die Benutzern und Gruppen pro Gerätekategorie, Schnittstelle oder einem einzelnen Gerät zugewiesen werden. |
| **Zeitlich begrenzter Zugriff** | Ein Zeitraum, in dem Benutzern der Zugriff auf Geräte und Schnittstellen auf kontrollierten Computern (wenn der Zugriff normalerweise blockiert wird) gewährt wird. |

# 15 Anhang 1 – Bereitstellungsfehlermeldungen

## 15.1 Einführung

Dieser Abschnitt beinhaltet eine Liste von Fehlern, die bei der Bereitstellung von Agenten oder Schutzrichtlinien auftreten können, deren mögliche Ursachen und mögliche Lösungen. Der Bereitstellungsstatus kann über die GFI EndPointSecurity-Verwaltungskonsole unter **Status ► Bereitstellung ► Bereitstellungsverlauf** abgerufen werden.

## 15.2 Bereitstellungsfehlermeldungen



Einige Fehlermeldungen in der Tabelle sind im Format „GFI EndPointSecurity-Fehler (Systemfehler)“. Die Fehler in Klammern werden vom System gemeldet und können je nach Fehlerursache variieren.

| Nachricht | Mögliche Ursache | Mögliche Lösung |
|---|---|---|
| **Der Computer ist offline.** | Die GFI EndPointSecurity-Verwaltungskonsole schickt bei der Bereitstellung einen Ping an den zu kontrollierenden Computer, um festzustellen, ob dieser online ist. Falls der Computer nicht online ist, wird diese Fehlermeldung angezeigt. | Falls ein zu kontrollierender Computer offline ist, erfolgt eine Stunde später automatisch ein erneuter Versuch. GFI EndPointSecurity versucht die Richtlinie so lange jede Stunde bereitzustellen, bis der zu kontrollierende Computer wieder online ist.<br>Stellen Sie sicher, dass der Zielcomputer eingeschaltet und mit dem Netzwerk verbunden ist. |
| **Verbindung mit Remote-Registry fehlgeschlagen. (Fehler)** | GFI EndPointSecurity konnte keine Daten aus der Registry des kontrollierten Computers extrahieren. | Stellen Sie sicher, dass Ihre Firewall-Einstellungen die Kommunikation zwischen kontrollierten Computern und dem GFI EndPointSecurity-Server zulassen. |
| **Erforderliche Informationen konnten nicht ermittelt werden. (Fehler)** | GFI EndPointSecurity konnte keine Versionsdaten des zu kontrollierenden Computer extrahieren (Version des Betriebssystems und der Agentenversion von GFI EndPointSecurity). | Verwenden Sie den Systemfehler (in Klammern) für weitere Details zur Fehlerursache und einer möglichen Lösung. |
| **Erstellen der erforderlichen Installationsdateien fehlgeschlagen. (Fehler)** | GFI EndPointSecurity konnte nicht die notwendigen Konfigurationsinformationen in die Bereitstellungsdatei (.msi-Installationsdatei) des GFI EndPointSecurity-Agenten einfügen. Dieser Fehler tritt auf, bevor die Bereitstellungsdatei auf den zu kontrollierenden Computer kopiert wird. | Verwenden Sie den Systemfehler (in Klammern) für weitere Details zur Fehlerursache und einer möglichen Lösung. |

| Nachricht | Mögliche Ursache | Mögliche Lösung |
|---|---|---|
| **Kopieren der Dateien zur Remote-Registry fehlgeschlagen. (Fehler)** | GFI EndPointSecurity konnte die Bereitstellungsdatei (.msi-Installationsdatei) nicht auf den zu kontrollierenden Computer kopieren.<br>Es kann sein, dass die administrative Freigabe (C$), die GFI EndPointSecurity für die Verbindung mit dem zu kontrollierenden Computer verwendet, deaktiviert ist. | Verwenden Sie den Systemfehler (in Klammern) für weitere Details zur Fehlerursache und einer möglichen Lösung.<br>Weitere Informationen zur Netzwerkkonnektivität und zu Sicherheitsberechtigungen finden Sie unter: **http://kbase.gfi.com/showarticle.asp?id=KBID003754** |
| **Zeitüberschreitung** | Die Bereitstellung des Agenten auf dem zu kontrollierenden Computer dauert entweder zu lange oder wird blockiert. | Versuchen Sie, den GFI EndPointSecurity-Agenten erneut bereitzustellen. |
| **Installation des Bereitstellungsdienstes fehlgeschlagen. (Fehler)** | Der GFI EndPointSecurity-Agent konnte aufgrund eines ausgeführten Dienstes auf dem zu kontrollieren Computer nicht installiert/deinstalliert werden. | Verwenden Sie den Systemfehler (in Klammern) für weitere Details zur Fehlerursache und einer möglichen Lösung. |
| **Installation fehlgeschlagen.** | Die Installation des GFI EndPointSecurity-Agenten wurde abgeschlossen, wird aber nicht als installiert in der Registry gekennzeichnet.<br>Die Versions- und Build-Nummer des GFI EndPointSecurity-Agenten entsprechen nicht der Versions- und Build-Nummer der GFI EndPointSecurity-Verwaltungskonsole. | Konsultieren Sie die Installationsprotokolldateien auf dem zu kontrollierenden Computer für weitere Details zur Fehlerursache und einer möglichen Lösung: %windir%\EndPointSecurity. |
| **Deinstallation fehlgeschlagen.** | Die Deinstallation des GFI EndPointSecurity-Agenten wurde abgeschlossen, wird aber nicht als deinstalliert in der Registry gekennzeichnet. | Konsultieren Sie die Installationsprotokolldateien auf dem zu kontrollierenden Computer für weitere Details zur Fehlerursache und einer möglichen Lösung: %windir%\EndPointSecurity. |
| **Der Vorgang ist aufgrund einer ungekannten Ausnahme fehlgeschlagen.** | GFI EndPointSecurity hat einen unerwarteten Fehler erkannt. | Verwenden Sie den Fehlerbehebungsassistenten, um den technischen Support von GFI zu kontaktieren.<br>Den Fehlerbehebungsassistenten finden Sie unter **Start ► Programme ► GFI EndPointSecurity 4.3 ► GFI EndPointSecurity 4.3-Fehlerbehebungsassistent**. |

# Inhalt

### USA, CANADA, CENTRAL AND SOUTH AMERICA

15300 Weston Parkway, Suite 104, Cary, NC 27513, USA

Telephone: +1 (888) 243-4329

Fax: +1 (919) 379-3402

Email: ussales@gfi.com

### UK AND REPUBLIC OF IRELAND

Magna House, 18-32 London Road, Staines, Middlesex, TW18 4BP, UK

Telephone: +44 (0) 870 770 5370

Fax: +44 (0) 870 770 5377

Email: sales@gfi.co.uk

### EUROPE, MIDDLE EAST AND AFRICA

GFI House, San Andrea Street, San Gwann, SGN 1612, Malta

Telephone: +356 2205 2000

Fax: +356 2138 2419

Email: sales@gfi.com

### AUSTRALIA AND NEW ZEALAND

83 King William Road, Unley 5061, South Australia

Telephone: +61 8 8273 3000

Fax: +61 8 8273 3099

Email: sales@gfiap.com